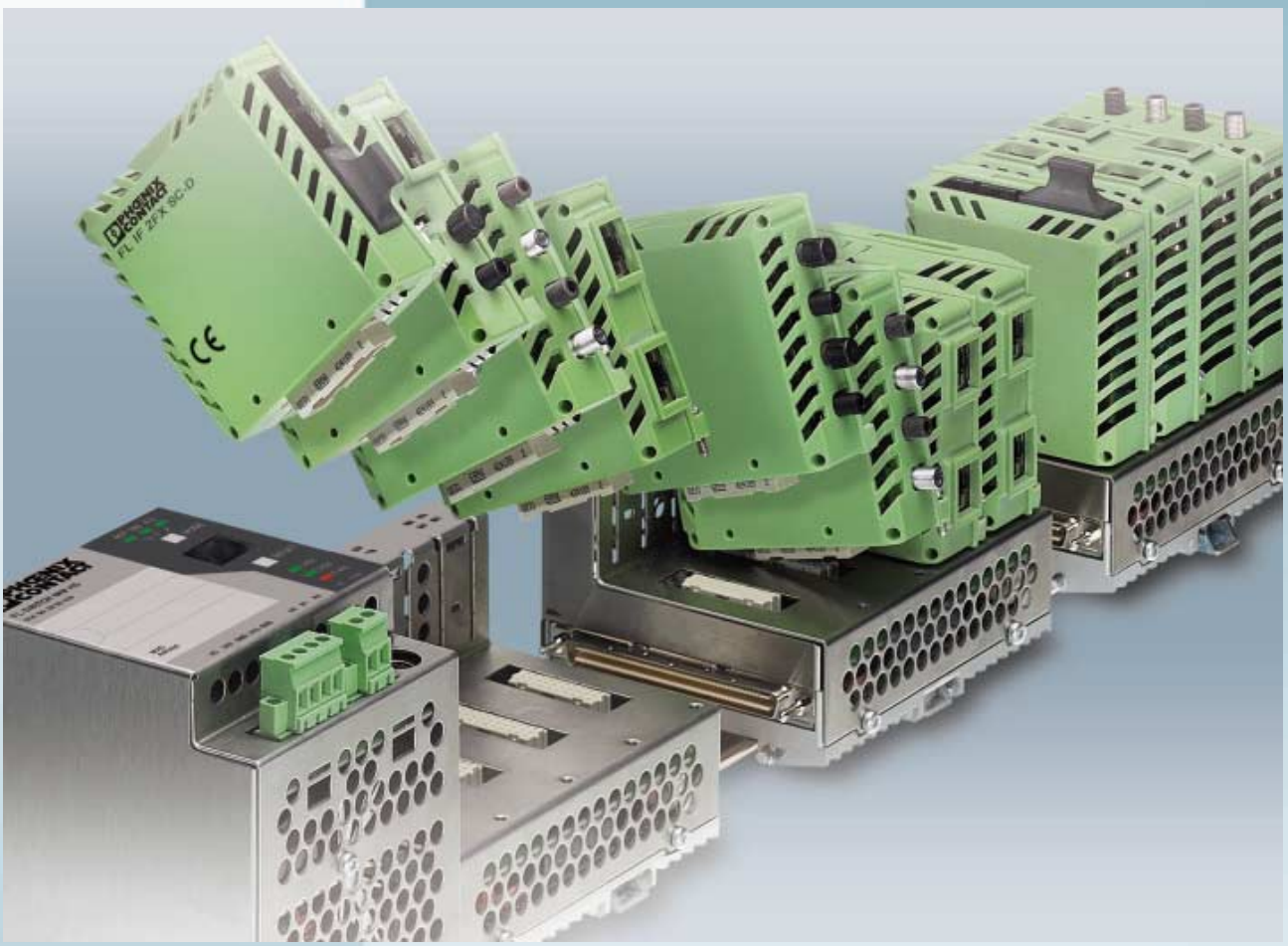
AUTOMATIONWORX



User Manual

FL SWITCH MM HS UM E

Order No. 2699011

Modular Managed Switch System

PHOENIX CONTACT
INSPIRING INNOVATIONS

AUTOMATIONWORX

User Manual

Description of the Hardware and Software Functions of the Modular Managed Switch System With Firmware Version 4.50

11/2006

Designation: FL SWITCH MM HS UM E

Revision: 09

Order No.: 2699011

This user manual is valid for:

The Modular Managed Switch System with firmware Version 4.50 from the Factory Line product range.

The Modular Managed Switch System includes:
- The FL SWITCH MM HS and FL SWITCH MM HS/M head stations
- The FL MXT and FL MXT/M extension modules
- The various FL IF ... interface modules

Please Observe the Following Notes

In order to ensure the safe use of the product described, we recommend that you read this manual carefully. The following notes provide information on how to use this manual.

User Group of This Manual

The use of products described in this manual is oriented exclusively to qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.

Phoenix Contact accepts no liability for erroneous handling or damage to products from Phoenix Contact or third-party products resulting from disregard of information contained in this manual.

Explanation of Symbols Used

The *attention* symbol refers to an operating procedure which, if not carefully followed, could result in damage to hardware and software or personal injury.

The *note* symbol informs you of conditions that must be strictly observed to achieve error-free operation. It also gives you tips and advice on the efficient use of hardware and on software optimization to save you extra work.

The *text* symbol refers to detailed sources of information (manuals, data sheets, literature, etc.) on the subject matter, product, etc. This text also provides helpful information for the orientation in the manual.

We Are Interested in Your Opinion

We are constantly striving to improve the quality of our manuals.

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send us your comments.

PHOENIX CONTACT GmbH & Co. KG
Documentation Services
32823 Blomberg
Germany

Phone +49 - (0) 52 35 30 0
Fax +49 - (0) 52 35 34 18 08
E-mail tecdoc@phoenixcontact.com

General Terms and Conditions of Use for Technical Documentation

Phoenix Contact GmbH & Co. KG reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular data sheets, installation instructions, manuals, etc.) does not constitute any further duty on the part of
Phoenix Contact GmbH & Co. KG to furnish information on alterations to products and/or technical documentation. Any other agreement shall only apply if expressly confirmed in writing by Phoenix Contact GmbH & Co. KG.
Please note that the supplied documentation is product-specific documentation only and that you are responsible for checking the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations.
Although Phoenix Contact GmbH & Co. KG makes every effort to ensure that the information content is accurate, up-to-date, and state-of-the-art, technical inaccuracies and/or printing errors in the information cannot be ruled out. Phoenix Contact GmbH & Co. KG does not offer any guarantees as to the reliability, accuracy or completeness of the information.
All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

Phoenix Contact GmbH & Co. KG accepts no liability or responsibility for errors or omissions in the content of the technical documentation (in particular data sheets, installation instructions, manuals, etc.).

The aforementioned limitations of liability and exemptions from liability do not apply, in so far as liability must be assumed, e.g., according to product liability law, in cases of premeditation, gross negligence, on account of loss of life, physical injury or damage to health or on account of the violation of important contractual obligations. Claims for damages for the violation of important contractual obligations are, however, limited to contract-typical, predictable damages, provided there is no premeditation or gross negligence, or that liability is assumed on account of loss of life, physical injury or damage to health. This ruling does not imply a change in the burden of proof to the detriment of the user.

Statement of Legal Authority

This manual, including all illustrations contained herein, is copyright protected. Use of this manual by any third party is forbidden. Reproduction, translation, and public disclosure, as well as electronic and photographic archiving or alteration requires the express written consent of Phoenix Contact. Violators are liable for damages.

Phoenix Contact reserves all rights in the case of patent award or listing of a registered design. Third-party products are always named without reference to patent rights. The existence of such rights shall not be excluded.

Internet

Up-to-date information on Phoenix Contact products can be found on the Internet at:

www.phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:

www.download.phoenixcontact.com

A conversion table is available on the Internet at:

www.download.phoenixcontact.com/general/7000_en_00.pdf

Table of Contents

1 Modular Managed Switch System 1-1

1.1 Properties 1-1
1.1.1 System Components 1-3
1.1.2 Firmware Versions and Their Functions 1-5
1.1.3 Firmware Functions and the Required Hardware 1-6
1.1.4 Dimensions of the Modular Managed Switch System for Normal Operation 1-10
1.1.5 Dimensions of the Modular Managed Switch System for GL-Certified Operation 1-11
1.1.6 Assignment of Ports to Slots 1-12
1.2 Status and Diagnostic Indicators 1-12
1.2.1 LEDs on the Head Station and Extension Modules 1-12
1.2.2 Meaning of the 7-Segment Display 1-14

2 Assembly and Installation 2-1

2.1 Assembly and Removal of the Head Station 2-1
2.2 Assembly and Removal of Extension Modules 2-3
2.3 Assembly and Removal of Interface Modules 2-5
2.4 Assembly and Removal of the FL M LABEL Labeling Field (Accessories) 2-7
2.4.1 Assembly 2-7
2.4.2 Removal 2-8
2.4.3 Dimensions of the Labeling Field 2-8
2.5 Installing the Modular Managed Switch System 2-9
2.5.1 Connecting the Supply Voltage to the FL SWITCH MM HS Head Station 2-9
2.5.2 Connecting the Supply Voltage to the FL SWITCH MM HS/M for GL-Certified Operation 2-10
2.5.3 Alarm Contact 2-11
2.5.4 V.24 (RS-232) Interface for External Management 2-12
2.6 Grounding 2-12

3 Startup and Functions 3-1

3.1 Basic Settings 3-1
3.1.1 Default Upon Delivery/Default Settings 3-1
3.1.2 Assigning IP Parameters 3-2
3.1.3 Flowchart After a Restart 3-7
3.2 Starting Up Interface Modules 3-9
3.2.1 FL IF 2TX VS-RJ 3-9
3.2.2 FL IF 2POF 10/100 3-11
3.2.3 FL IF 2HCS 100 3-14
3.2.4 FL IF 2FX SC .../FL IF 2FX SM SC 3-16

3.2.5 FL IF 2FX ST-D ... 3-18
3.2.6 FL IF TX/POF 10/100 3-19
3.2.7 FL IF TX/HCS 100 3-20
3.2.8 FL IF MEM 2TX-D ... 3-22
3.2.9 FL IF 2PSE-F ... 3-24
3.2.10 FL IF 2POF SCRJ-D ... 3-28
3.3 Frame Switching ... 3-31
3.3.1 Store-and-Forward ... 3-31
3.3.2 Multi-Address Function ... 3-31
3.3.3 Learning Addresses ... 3-31
3.3.4 Prioritization ... 3-32

4 Configuration and Diagnostics ... 4-1
4.1 Factory Manager ... 4-1
4.1.1 General Function ... 4-1
4.1.2 Assigning IP Parameters ... 4-1
4.1.3 Configuration and Diagnostics ... 4-3
4.2 Web-Based Management (WBM) ... 4-11
4.2.1 General Function ... 4-11
4.2.2 Requirements for the Use of WBM ... 4-11
4.2.3 Functions/Information in WBM ... 4-12
4.3 Simple Network Management Protocol (SNMP) ... 4-41
4.3.1 General Function ... 4-41
4.3.2 Diagram of SNMP Management ... 4-44
4.3.3 RFC1213 MIB - MIB II ... 4-46
4.3.4 RMON MIB (1.3.6.1.2.1.16) ... 4-53
4.3.5 Bridge MIB (1.3.6.1.2.1.17) ... 4-59
4.3.6 pBridgeMIB (1.3.6.1.2.1.17.6) ... 4-61
4.3.7 qBridgeMIB (1.3.6.1.2.1.17.7) ... 4-62
4.3.8 rstp MIB (1.3.6.1.2.1.17.11) ... 4-65
4.3.9 IANAifType MIB (1.3.6.1.2.1.30) ... 4-66
4.3.10 IF MIB (1.3.6.1.2.1.31) ... 4-66
4.3.11 Private MIBs ... 4-69
4.4 Management via Local V.24 (RS-232) Communication Interface ... 4-116
4.4.1 General Function ... 4-116
4.4.2 User Interface Functions ... 4-117
4.4.3 Starting With Faulty Software (Firmware) ... 4-120
4.5 Management via Telnet ... 4-123
4.5.1 Configuring the Telnet Terminal ... 4-123
4.5.2 Telnet Interface Functions ... 4-123

5 (Rapid) Spanning Tree ... 5-1
5.1 General Function ... 5-1
5.2 (R)STP Startup ... 5-2

5.2.1 Enabling (R)STP on All Switches Involved 5-2
5.2.2 Connection Failure - Example 5-11
5.2.3 Mixed Operation of RSTP and STP 5-12
5.2.4 Topology Detection of a Rapid Spanning Tree Network (RSTP) 5-12
5.2.5 Configuration Notes for Rapid Spanning Tree 5-15

6 Multicast Filtering 6-1
6.1 Basics 6-1
6.2 Enabling the Web Pages for Multicast Filtering in WBM 6-1
6.3 Static Multicast Groups 6-1
6.3.1 "Current Multicast Groups" Web Page 6-2
6.3.2 Creating Static Multicast Groups 6-2
6.3.3 Procedure for Creating a Multicast Group 6-5
6.4.1 Internet Group Management Protocol (IGMP) 6-7
6.4.2 "General Multicast Configuration" Web Page 6-8

7 Virtual Local Area Network (VLAN) 7-1
7.1 Basics 7-1
7.2 Enabling the VLAN Web Pages in Web-Based Management 7-1
7.2.1 Management VLAN ID 7-2
7.2.2 Changing the Management VLAN ID 7-2
7.3 General VLAN Configuration 7-3
7.4 Current VLANs 7-4
7.4.1 Static VLANs 7-5
7.4.2 VLAN Port Configuration 7-6
7.4.3 VLAN Port Configuration Table 7-7
7.5 Creating Static VLANs 7-7
7.5.1 Dynamic Configuration 7-9
7.6 VLAN and (R)STP 7-9

8 Operating as a PROFINET Device 8-1
8.1 Preparing the Switch for PROFINET Mode 8-1
8.2 Switch as a PROFINET IO Device 8-2
8.2.1 Configuration in the Engineering Tool 8-2
8.2.2 Configuring the Switch as a PROFINET IO Device 8-4
8.2.3 PROFINET Flashing Function 8-5
8.2.4 Naming the Device 8-5
8.2.5 Operating in the PROFINET Environment 8-5
8.3 PROFINET Alarms 8-6
8.3.1 Alarms in WBM 8-6

9 LLDP (Link Layer Discovery Protocol) 9-1

9.1 Basics 9-1

9.2 Representation of the Topology in an Engineering Tool 9-4

10 DHCP Relay Agent 10-1

10.1 Activating the DHCP Relay Agent 10-1

11 Technical Data and Ordering Data 11-1

11.1 Technical Data 11-1

11.2 Typical MMS Current Consumption (Example) 11-5

11.3 Ordering Data 11-7

11.4 Ordering Data for GL-Certified Components (GL Certificate No. 24 2750 4 HH) 11-8

1 Modular Managed Switch System

Unless stated otherwise, all information in this manual is valid for the FL SWITCH MM HS and FL SWITCH MM HS/M, as well as for the FL MXT and FL MXT/M.

1.1 Properties

The **M**odular **M**anaged **S**witch (**Modular Managed Switch System - MMS**) is an Ethernet switch, which is suitable for industrial use and consists of a head station, extension modules, and interface modules. The head station and extension modules contain the entire Ethernet switching technology. Interface modules provide the interface to the desired physical transmission method. An extension module can be used to extend the head station from eight ports to 16 ports, and the use of two extension modules gives a maximum of 24 ports. The desired transmission medium can be freely selected using the various interface modules.

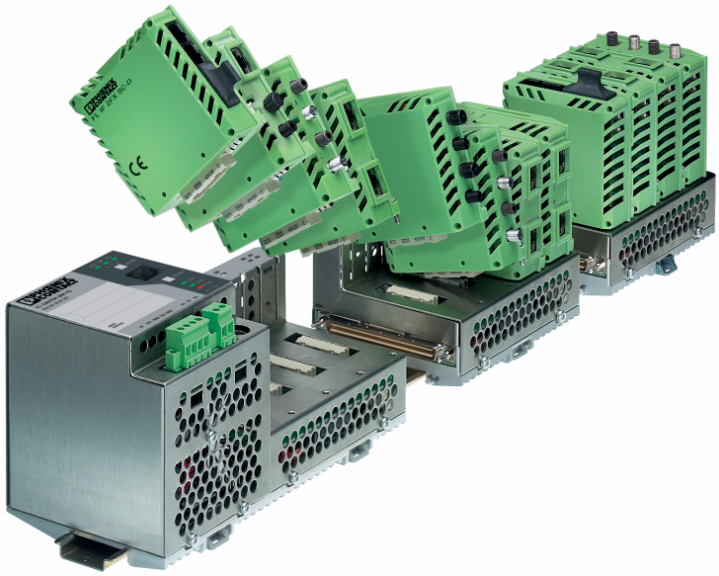


Figure 1-1 The Modular Managed Switch System

Future-Proof Networks for the Highest Possible Requirements

Transmission method

10/100 Mbps polymer/HCS fibers
Easy to assemble polymer fibers can now also be used for Ethernet. This cost-effective fiber optic technology can cover distances of up to 50 m. This provides cost savings both during installation and for maintenance when replacing mechanically damaged fiber optic cables.
HCS fiber technology is available for distances of up to 100 m.

Maximum availability

Maximum network availability
A device design that does not use a fan, the redundant power supply, and conformance with all relevant industrial standards in terms of EMC, climate, mechanical load, etc. ensure the highest possible level of availability.
Redundancy can also be created with standards: the (Rapid) Spanning Tree Protocol ensures the safe operation of the entire network regardless of topology, even in the event of a cable interrupt.

All information

Clear Information
You can label your device clearly using the large labeling field, and read operating states and additional information from the two-digit 7-segment display. Two LEDs per port with switchable information ensure that you always have sufficient local information. A web server and an SNMP agent are provided for diagnostics, maintenance, and configuration via the network. A terminal access point can be used for local operation.

Port mirroring

Port mirroring can be used to monitor data traffic on the network connections.

Modularity

Modular structure
Depending on your requirements, you can create a compact switch for the control cabinet (with convenient connections on the front) or a switch for the terminal box (with connections at the bottom). It is also possible to add a glass fiber interface or extend your existing station from 8/16 ports to a maximum of 24 ports.

Figure 1-2 Possible system hardware

Features and Fields of Application of the FL SWITCH MM HS

- Increased network performance by filtering data traffic:
  - Local data traffic remains local.
  - The data volume in the network segments is reduced.
- Easy network expansion and network configuration.
- Coupling segments with different transmission speeds.
  Automatic detection of 10 Mbps or 100 Mbps data transmission rate with auto crossing.
- Increased availability through the use of redundant transmission paths with Rapid Spanning Tree. Support of various topologies and meshed structures as well as ring topologies with special ring detection. Fast switch-over times with RSTP fast ring detection.
- Configuration of switches using web-based management, SNMP, Telnet or locally via a V.24 (RS-232) interface.
- Multicast filtering (static and dynamic).
- IGMP snooping, optional querier function.
- VLAN support according to 802.1Q (32 VLANs).
- Port security functions.
- Access control for web-based management (WBM).
- Integration in PROFINET environments.
- Topology detection using LLDP (Link Layer Discovery Protocol).
- Address assignment via BootP, DHCP, DCP or statically.
- Address assignment using DHCP option 82 relay agent.
- Support of Power over Ethernet (PoE).

1.1.1 System Components

Central element FL SWITCH MM HS

The head station is the central element of the Modular Managed Switch System. It contains all the management functions, and the interface modules provide it with the desired interfaces to the network. Up to two extension modules can be connected to a head station, which means that the maximum system configuration comprises 24 Ethernet ports.

FL SWITCH MM HS/M

Thanks to certification according to Germanischer Lloyd (GL Certificate No. 2427504 HH), the FL SWITCH MM HS/M head station, the FL MXT/M extension module, and some of the available interface modules have been approved for shipbuilding and off/onshore applications. Please observe the list of GL-certified components on page 11-8. Please also observe the notes for supply voltage connection on page 2-10.

Always switch off the supply voltage before inserting or removing extension modules (FL MXT).

Do not connect more than two extension modules (FL MXT) to one head station.

Extension module FL MXT

An extension module provides another 8 ports, which can be individually equipped with interface modules. A maximum of 2 extension modules can be connected to the head station. The maximum system configuration therefore comprises 24 ports.

It is not possible to operate the extension modules without the head station.

FL MXT/M

The FL MXT/M extension module is approved for shipbuilding and off/onshore applications thanks to its certification according to GL (Certificate No. 2427504 HH).

Interface modules FL IF ...

Please observe the list of GL-certified components on page 11-8.

Interface modules provide the desired interface to the network. The two outlet directions, the various types of media supported, and the port density of two ports per interface module provide a high degree of flexibility in terms of the system configuration.

Converter board FL CB IF

When connected to the FL CB IF converter board, the FL IF TX/POF-... interface module can be used as a stand-alone media converter.

Figure 1-3 FL CB IF converter board

1.1.2 Firmware Versions and Their Functions

Firmware Version 1.03 provides the standard switch functions.

In addition, firmware Version 1.11 supports the Spanning Tree redundancy mechanism.

Firmware 2.03 offers the following additional functions:

– Multicast filter mechanisms
– IGMP snooping and querier function
– Memory module support

Firmware 2.10 offers the following additional functions:

– Auto-refresh of various WBM pages
– POF and FX interface module support
– Extensive support and improved configuration handling of the memory module
– Extended multicast filtering (multicast transmitters are detected and added to multicast groups)
– Extended IGMP snooping and IGMP query function (switch passively reads IGMP membership reports, creates corresponding multicast groups, and sends IGMP queries to multicast groups)
– Visualization of port capacity
– Port prioritization

Firmware 3.04 offers the following additional functions:

– VLAN support
– Rapid Spanning Tree support
– Security options (port-based security and access control for WBM)
– Optimization of the password concept
– Event table (logging of important events)
– Representation of MAC address table in WBM

Firmware 4.03 offers the following additional functions:

– Optimized Rapid Spanning Tree Protocol (RSTP) (improved switch-over times)
– Fast ring detection
– Large tree support
– Support of LLDP topology detection
– DHCP support
– DHCP with option 82 relay agent
– PROFINET device function and DCP
– Support of Power over Ethernet (IEEE 802.3af)
– Simplified port configuration
– IGMP query Version 1 and 2

Firmware 4.50 offers the following additional functions:

– Support of the POF-SCRJ interface module and corresponding diagnostics
– SNMP traps can be disabled individually
– The VLAN for management can be set: VLAN ID to manage (web, SNMP, ping, IGMP query) the switch in "VLAN Tagging" mode
– DHCP relay agent can be disabled according to the port
– PROFINET alarms and configuration comparison
– Fast aging on link down

– Extended LED diagnostics (identification of the switch in the PROFINET environment and detection of the "Missing IP parameter following restart" status)
– PoE traps (when the PoE status changes)
– Test traps to check communication
– Deletion of the MAC address table from WBM and SNMP

1.1.3 Firmware Functions and the Required Hardware

Table 1-1 Functions and the required hardware

Function	Required Hardware for the Head Station	Required Hardware for the Extension Modules
Standard switch functions	Hardware Version ≥ 3 (includes system bus Version 4.1)	Hardware Version ≥ 2 (includes system bus Version 3.1)
Memory module support	Hardware Version ≥ 4 (includes system bus Version 4.2)	Hardware Version ≥ 2 (includes system bus Version 3.1)
PoE module support	Hardware Version ≥ 6 (includes system bus Version 5.0)	Hardware Version ≥ 4 (includes system bus Version 4.0)
POF-SCRJ module support	Hardware Version ≥ 6 (includes system bus Version 5.0)	Hardware Version ≥ 4 (includes system bus Version 4.0)

1.1.3.1 Front View of the Head Station

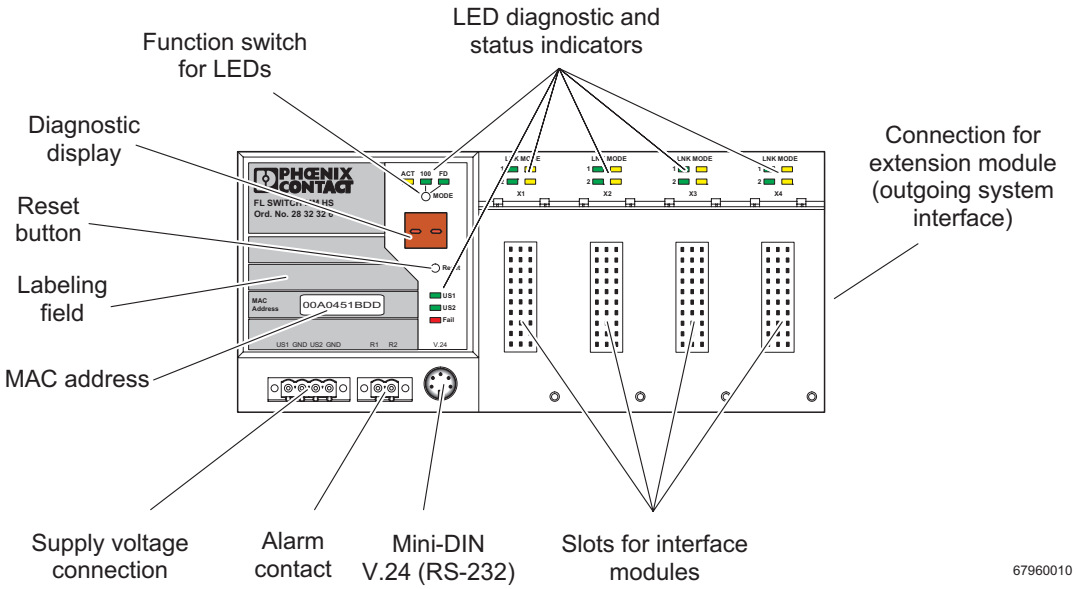


Figure 1-4 Front view of the head station

– Diagnostic/status indicators
  Important information is displayed directly on the device. Each port has two LEDs. The left-hand LED always indicates the "LINK", while the right-hand LED display is set with the function switch.
– Function switch for LEDs
  The MODE function switch can be used to specify which information is displayed by the second port-specific LED. The three LEDs above the switch indicate the selected mode. This information is then displayed by all port-specific LEDs (see also example on page 1-13).
– Connection for extension module (FL MXT)
  Connect the first of a maximum of two extension modules here.
– Slots for interface modules
  This is where the various interface modules (each with two ports) are inserted and locked in place.
– Mini-DIN V.24 (RS-232)
  V.24 (RS-232) interface in Mini-DIN format for local configuration via the serial interface.
– Alarm contact
  The floating alarm contact can be connected here via a 2-pos. COMBICON connector.
– Supply voltage connection
  The supply voltage can be connected via the 4-pos. COMBICON connector (redundancy is optional).
– Reset button

In order to prevent an accidental MMS reset, the reset button must be held down for a few seconds before it triggers a reset.

– Diagnostic display
  Various operating states or error states can be displayed here. For a list of possible codes, please refer to page 1-14.

1.1.3.2 Front View of the Extension Module

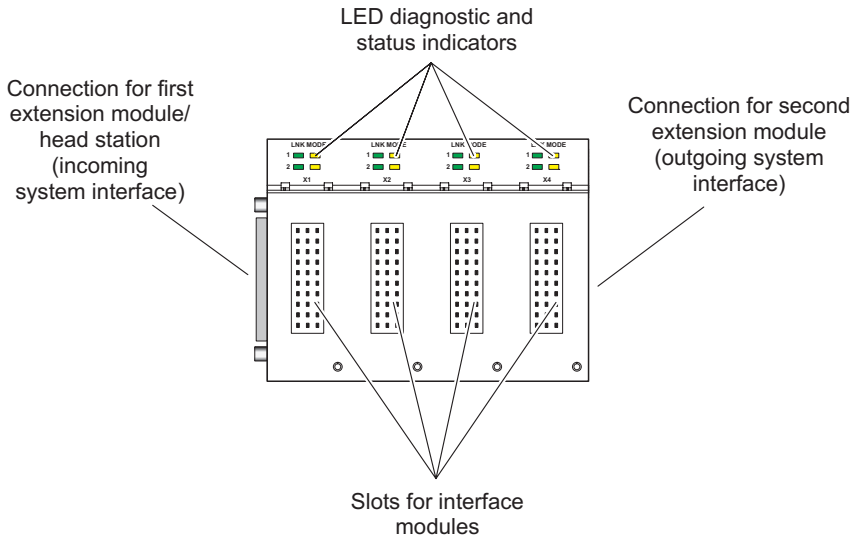


Figure 1-5 Front view of the extension module

– Diagnostic/status indicators
  Important information is displayed directly on the device.
– Connection for second extension module
  Connect the second extension module here.
– Connection for interface modules
  This is where the various interface modules are inserted and locked in place.
– Slot for first extension module/head station
  Connect this extension module either to a head station or to the first extension module here.

1.1.3.3 View of the Interface Modules (Example)

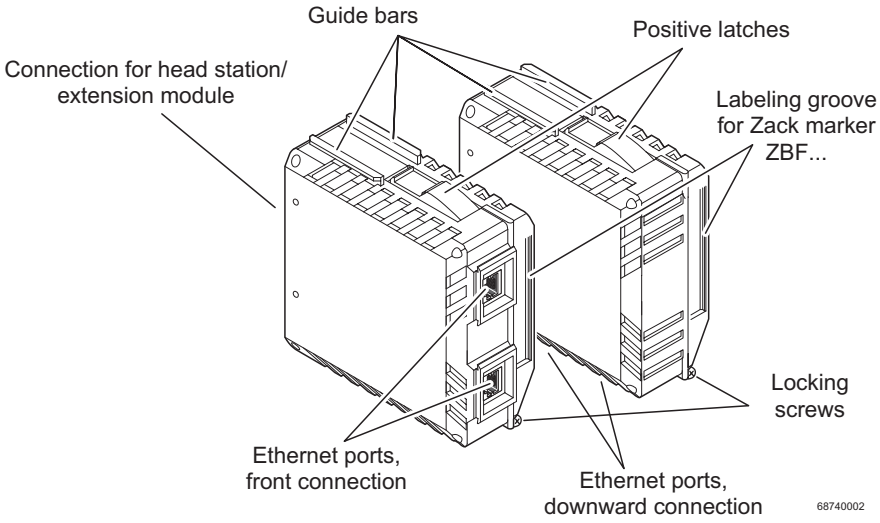


Figure 1-6 View of the interface modules (example)

– Connection for extension module/head station
  This connector is used to connect the interface module and the extension module or the head station.
– Guide bars
  These bars aid installation and hold the interface modules securely in place.
– Positive latches
  These latches must be pressed in order to remove the interface module (previous versions used mounting screws).
– Ethernet ports
  These are the ports for the various interfaces and connection directions.
– Marking groove for Zackband ZBF ...
– Mounting screws to lock the interface modules in place.

1.1.4 Dimensions of the Modular Managed Switch System for Normal Operation

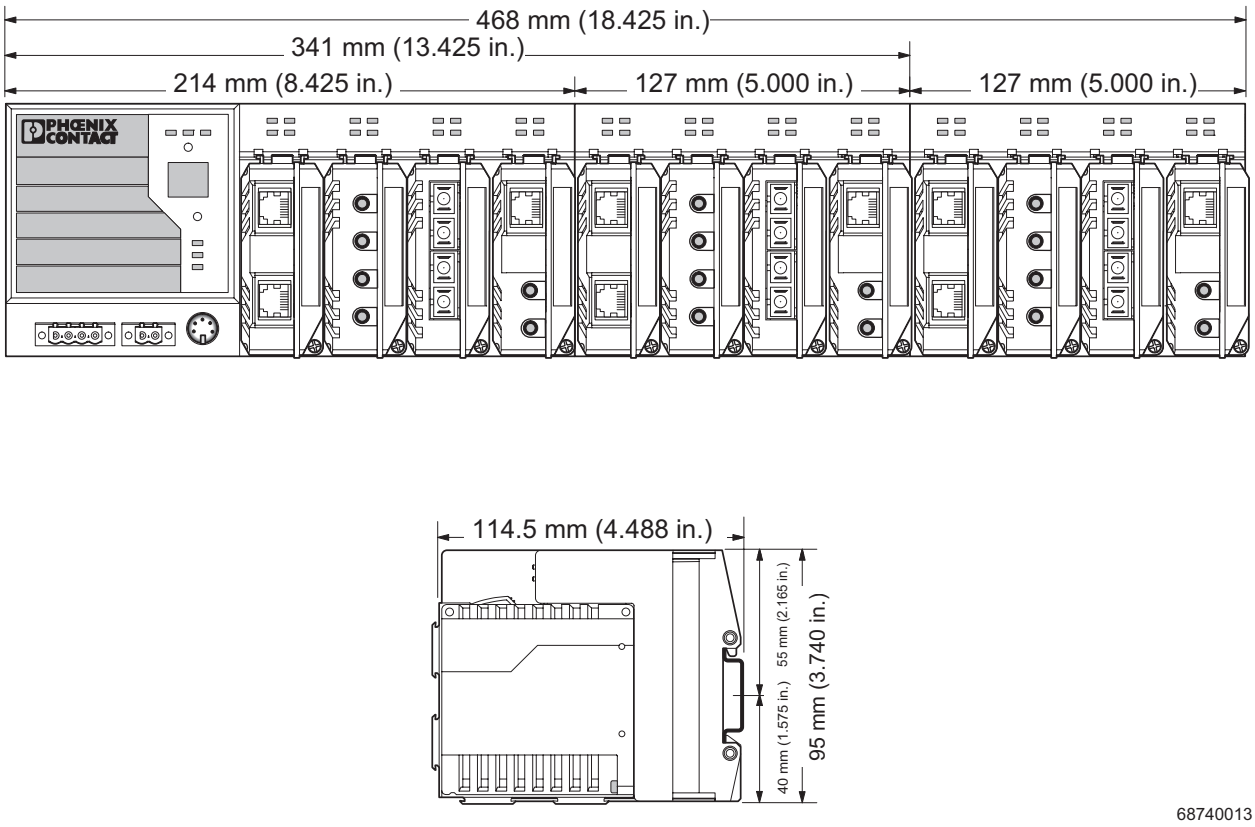


Figure 1-7 MMS housing dimensions in millimeters

1.1.5 Dimensions of the Modular Managed Switch System for GL-Certified Operation

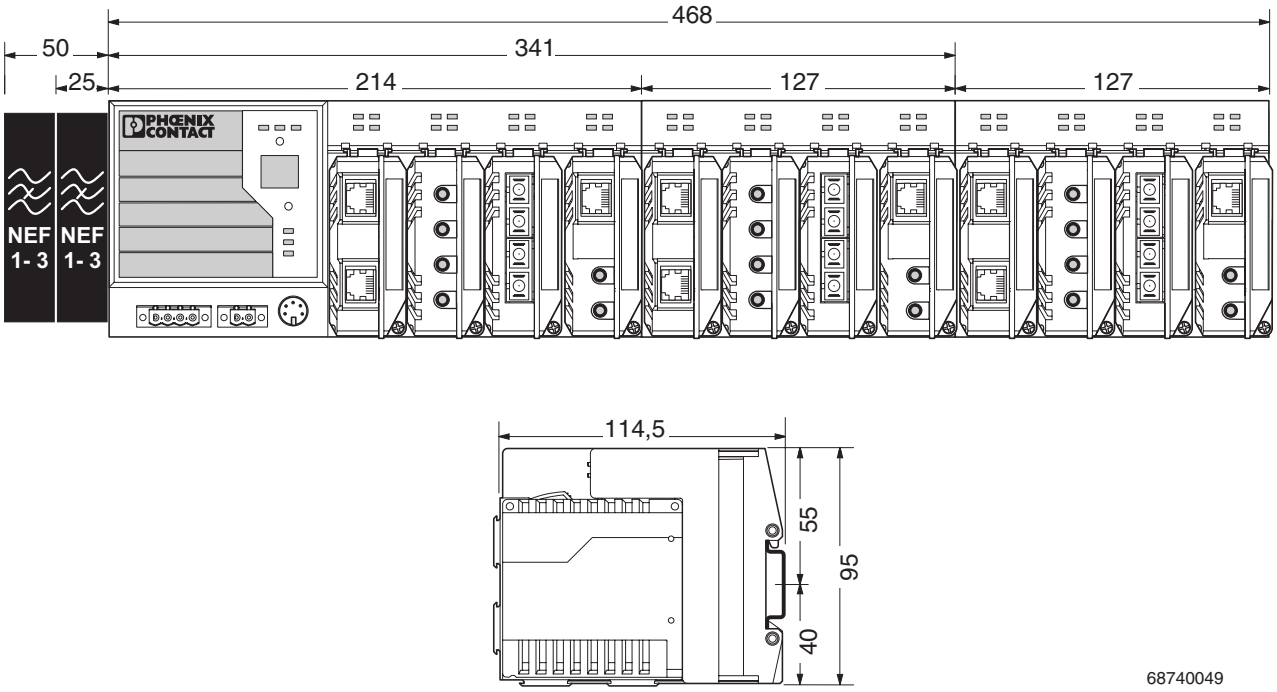
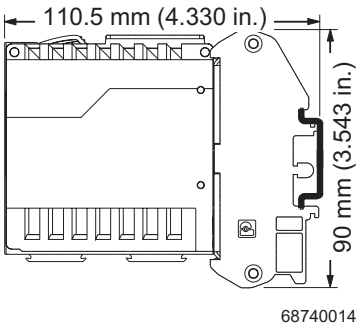


Figure 1-8 MMS housing dimensions in millimeters

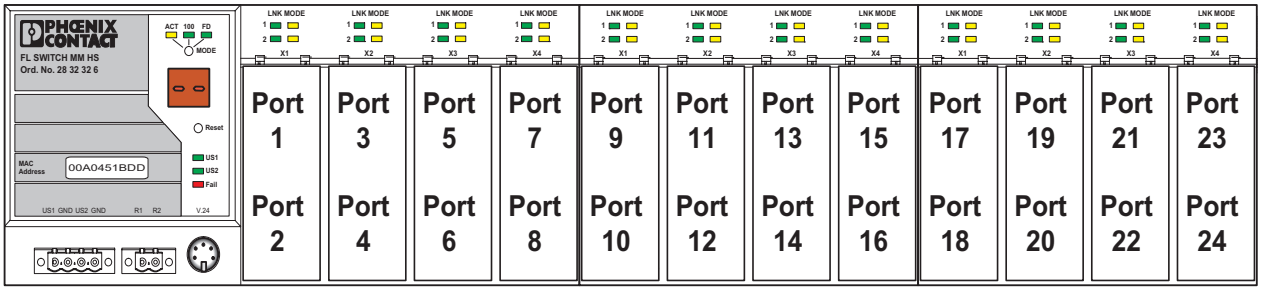
Housing Dimensions of the Converter Board With Interface Module



Housing width: 67 mm

Figure 1-9 Housing dimensions of the FL CB IF converter board

1.1.6 Assignment of Ports to Slots



68740028

Figure 1-10 Assignment of ports to slots

1.2 Status and Diagnostic Indicators

1.2.1 LEDs on the Head Station and Extension Modules

Des.	Color	Status	Meaning
US1	Green	ON	Supply voltage 1 in the tolerance range
		OFF	Supply voltage 1 too low
US2	Green	ON	Supply voltage 2 in the tolerance range
		OFF	Supply voltage 2 too low
FAIL	Red	ON	Alarm contact open, i.e., an error has occurred
		OFF	Alarm contact closed, i.e., an error has not occurred
A Link LED is located above the interface module slot for each port			
LNK (Link)	Green	ON	Link active
		OFF	Link inactive
A second LED is located above the interface module slot for each port. The function of the second LED (MODE) for each port can be set using a switch on the head station, which controls all ports (see also example below). There are three options:			
ACT (Activity)	Green	ON	Sending/receiving telegrams
		OFF	Not sending/receiving telegrams
100	Green	ON	100 Mbps
		OFF	10 Mbps if Link LED is active
FD (Duplex)	Green	ON	Full duplex
		OFF	Half duplex if Link LED is active
ACT and 100 and FD simultaneously	Green	Flashing	PROFINET device identification
ACT or 100 or FD (selected by mode switch)	Green	Flashing	No IP parameter present following restart

Example:

In Figure 1-11, the LED indicators have the following meaning (see also "Assignment of ports to slots" on page 1-12):

A: The switch has been set to display the duplex mode; the mode LEDs now indicate that port 1 and port 3 are in full duplex mode and port 2 and port 4 are in half duplex mode.

B: The switch has been set to display the data transmission rate; the mode LEDs now indicate that port 1 and port 2 are operating at 10 Mbps, port 3 is operating at 100 Mbps, and port 4 is not operating at all.

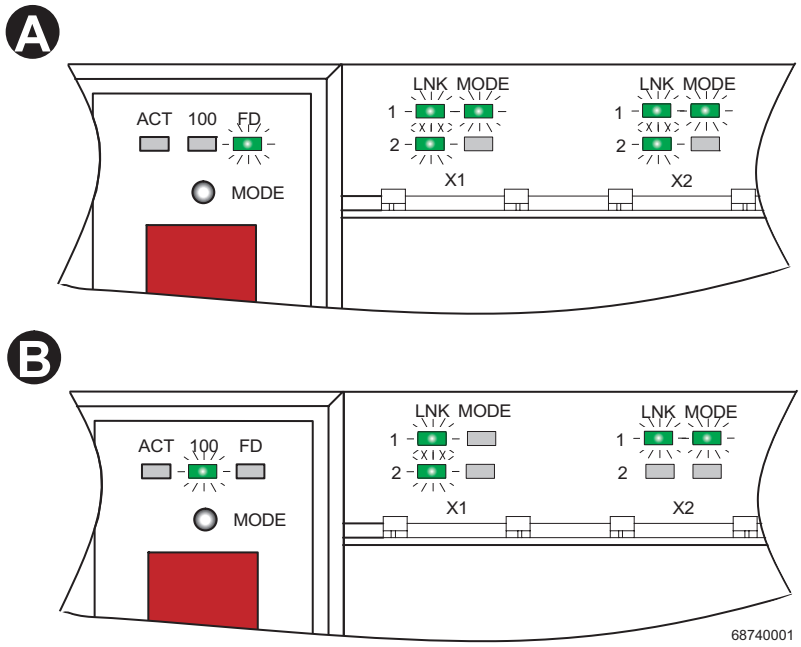


Figure 1-11 Example for status indicators

1.2.2 Meaning of the 7-Segment Display

If the MMS has established a PROFINET connection, a dot appears in the bottom-right corner of the display.

During Error-Free Operation:

Display	Meaning
bo	Extracting/starting firmware (boot)
01	Sending BootP requests
SC	Saving parameterization data to the plug-in memory and the head station.
03	Downloading firmware via TFTP
04	Loading firmware in the Flash memory that was loaded via the network
05	The recently loaded firmware was successfully saved in the Flash memory
_ _	Initializing firmware
--	Firmware running
rb	A reset has been triggered via SNMP, WBM or V.24 (RS-232), the device is preparing to restart (reboot)
rC	After a device configuration update, "**rC**" (reconfiguration) may appear in the display after a restart. This means that the firmware automatically adapts the new configuration and then restarts the switch again.
Pb	A port blocked by the port security function is indicated with "Pb".
dP	The device is operated as a PROFINET IO device and is waiting for startup using a PROFINET controller. The device cannot be accessed via an IP address.
"00" alternates with another display	In PROFINET mode, the engineering tool called the "flashing" function.
SP	Spanning Tree initialization active

Messages During Operation With the Memory Module:

Display	Meaning
0P	Parameterization data being read from the plug-in memory
EC	Equal configuration - the configurations on the memory module and in the head station are the same
dC	Different configuration - the configurations on the memory module and in the head station are different
0C	The memory module is empty

In the Event of an Error:

Display	Meaning	Remedy
16	The device software (firmware) is faulty	– Update the firmware via the serial interface.
17	Firmware transfer via TFTP or Xmodem failed (display changes from "03" to "17")	– Check the physical connection. – Establish a point-to-point connection. – Make sure that the file (with the specified file name) exists and is in the correct directory. – Check the IP address of the TFTP server. – Activate the TFTP server. – Repeat the download.
19	File transfer was completed successfully, but the file is not a valid firmware version for the Modular Managed Switch System	– Provide a valid firmware version with the previously specified file name (Internet: www.phoenixcontact.com). – Repeat the download.
80	An error has occurred in the firmware	– Restart the device (power up or reset). – Make sure that the IP address is not used more than once in the same network.
87	More than one parameterization memory has been plugged in	– Remove all but one of the memory modules and execute a reset.
89	The switch is or was in an exceptional situation	– Restart the device. – Check your network for configuration errors, loops, loose contacts, poor line quality, faulty network interfaces. – Make sure that there are no Denial of Service attacks.
Li	Link monitoring has detected at least one faulty link	– Check the cables/connectors. – In web-based management, check at which port link monitoring (see page 4-26) is indicating an error. – Restore the data connection to this port or deactivate link monitoring for this port. – Check the correct position of the interface module on the head station or on the extension module.
Cd	The switch is operating as a PROFINET IO device. The configuration of the switch and the configuration transmitted by the PROFINET engineering tool are different	– Set the desired configuration at the switch. – Modify the control program so that it contains the existing switch configuration.

Display	Meaning	Remedy
bF	System bus error (Bus Fail)	– Make sure that the extension modules are plugged in correctly. – Restart the switch.
Po	Power	– Power over Ethernet monitoring has been activated on at least one port and an error has occurred. Check the physical connection at the PoE ports and the settings in WBM.
HS	Hardware support	– At least one interface module is inserted in the MMS that is not fully supported by the MMS hardware version used. The interface module transmits data, the management functions are deactivated. The message appears for approximately ten seconds on the display after a restart or after interface modules have been inserted or removed. The interface module can be used in unmanaged mode.

The points under "Remedy" are recommendations, they do not all have to be carried out for every error.

For all other message codes that are not listed here, please contact Phoenix Contact.

2 Assembly and Installation

2.1 Assembly and Removal of the Head Station

Always switch off the supply voltage when assembling/removing the head station and extension modules.

Mount the head station on a clean DIN rail according to DIN EN 50 022 (e.g., NS 35 ... from Phoenix Contact). To avoid contact resistance only use clean, corrosion-free DIN rails. Before mounting the modules, an end clamp (E/NS 35N, Order No. 08 00 88 6) should be mounted on the left-hand side next to the head station to stop the modules from slipping on the DIN rail. The supplied ATP-ST-TWIN side cover (see "A" in Figure 2-4) and the end clamp should only be mounted on the right-hand side once the last extension module has been mounted.

Assembly:

1. Place the module onto the DIN rail from above (A). The upper holding keyway must be hooked onto the top edge of the DIN rail. Push the module from the front towards the mounting surface (B).

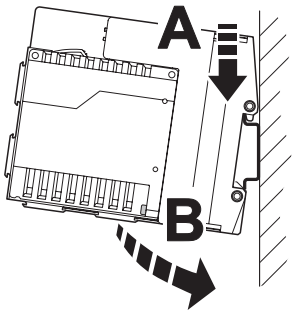


Figure 2-1 Snapping the head station onto the DIN rail

2. Once the module has been snapped on properly, check that it is fixed securely on the DIN rail. Check whether the positive latches are facing upwards, i.e., snapped on correctly.

Removal:

1. Remove all plug-in connections or interface modules.
2. Pull down the positive latches using a suitable tool (e.g., screwdriver). Both positive latches remain snapped out. Then swivel the bottom of the module away from the DIN rail slightly (A). Next, lift the module upwards away from the DIN rail (B).

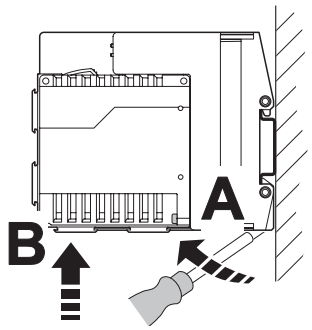


Figure 2-2 Removal of the head station

2.2 Assembly and Removal of Extension Modules

Always switch off the supply voltage when assembling/removing the extension modules.

Assembly:

1. Place the module onto the DIN rail from above (A). The upper holding keyway must be hooked onto the top edge of the DIN rail. Push the module from the front towards the mounting surface (B). Check that the positive latches have snapped on properly.

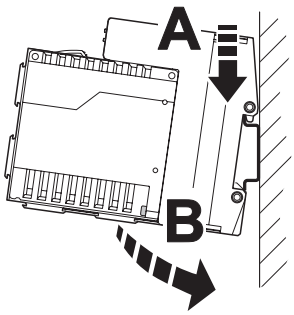


Figure 2-3 Assembly of extension modules

2. Now that the extension module is snapped onto the DIN rail, push it along the DIN rail towards the head station, until the male connector/female connector of the modules are interlatched and the sides of the modules lie flush with one another.

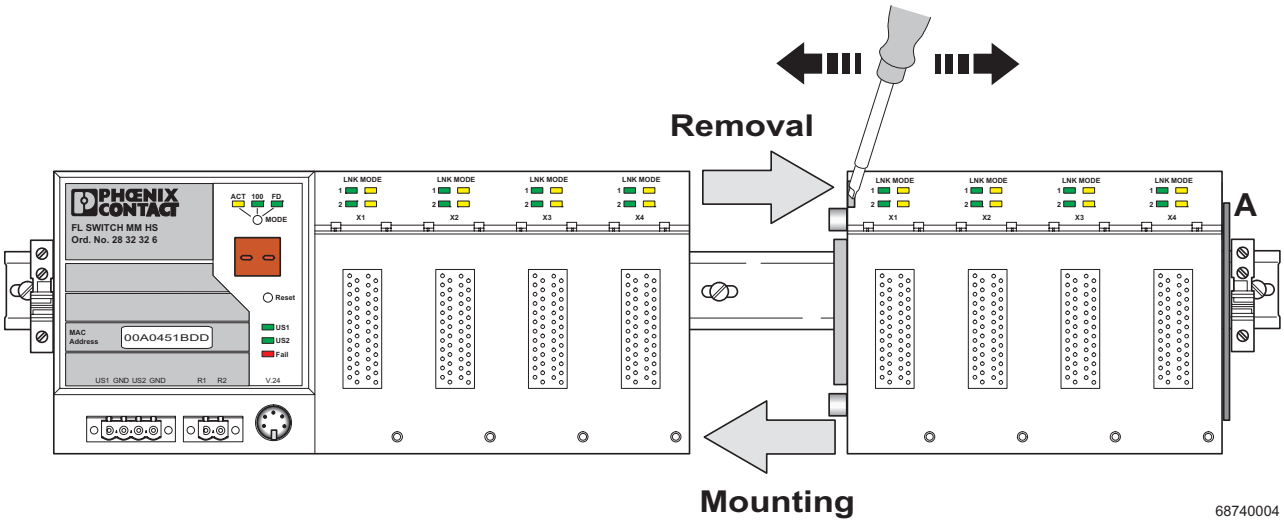


Figure 2-4 Assembly/removal of extension modules

Removal:

Switch off the supply voltage before removing the extension modules.

1. Remove all plug-in connections or interface modules.
2. To release the plug-in connection for the system interface, insert a screwdriver in the notch provided and use it to push the modules apart.
3. Push the right-hand extension module along the DIN rail to the right until the plug-in contact is completely free.
4. Pull down the holding latches using a suitable tool (e.g., screwdriver).
5. Then swivel the bottom of the module away from the DIN rail slightly (A). Next, lift the module upwards away from the DIN rail.

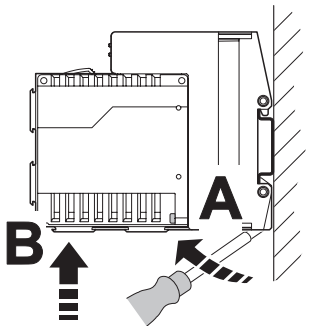


Figure 2-5 Removal of extension modules

2.3 Assembly and Removal of Interface Modules

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

Ensure that the surface of the head station or extension module housing is clean.

Assembly:

1. Insert the interface modules in the slots of the basic modules. The guide bars on the top of the interface modules must be pushed into the guide slots of the basic module without tilting them.

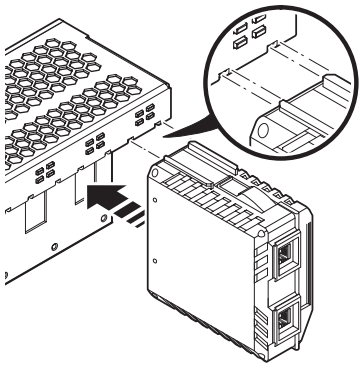


Figure 2-6 Assembly of interface modules

2. Now push the interface modules towards the basic module until the connector and the holding clamp are snapped into place.
3. Secure the interface module using the screw on the bottom right-hand side of the interface module.

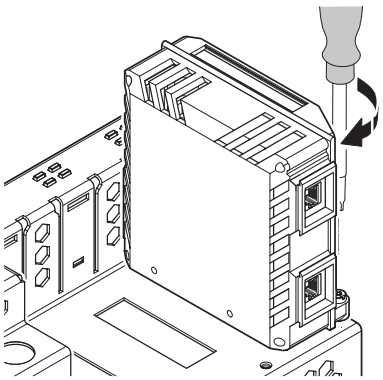


Figure 2-7 Securing the interface module

Removal:

1. Remove the mounting screw.

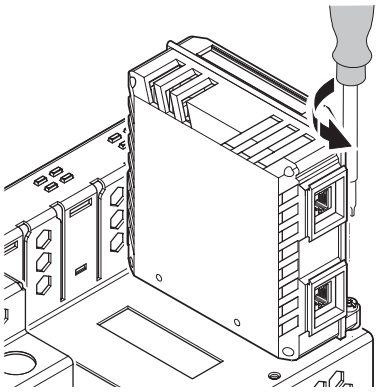


Figure 2-8 Removing the mounting screw on interface modules

2. Press the positive latch (A) and pull out the module (B).

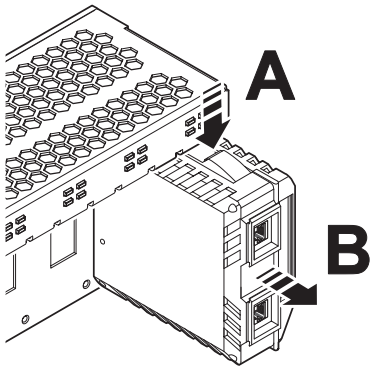


Figure 2-9 Removing the interface module

2.4 Assembly and Removal of the FL M LABEL Labeling Field (Accessories)

The FL M LABEL labeling field (Order No. 2891055) can be used to individually identify the ports of the MMS. The labeling field can be attached to the top of the head station or to the extension modules.

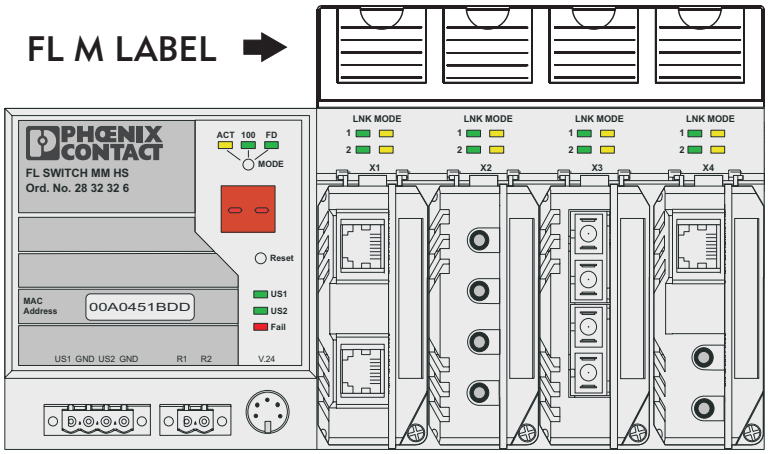


Figure 2-10 Head station with labeling field

2.4.1 Assembly

– Push the expansion plug through the mounting holes and into the openings on the top of the MMS (A).
– Press down on the expansion plug cap to secure the plug (B).

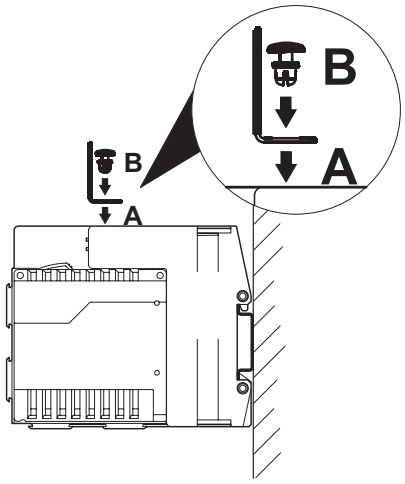


Figure 2-11 Assembly of the labeling field

2.4.2 Removal

– Pull the expansion plug cap upwards until the entire plug is removed.
– Remove the labeling field.

2.4.3 Dimensions of the Labeling Field

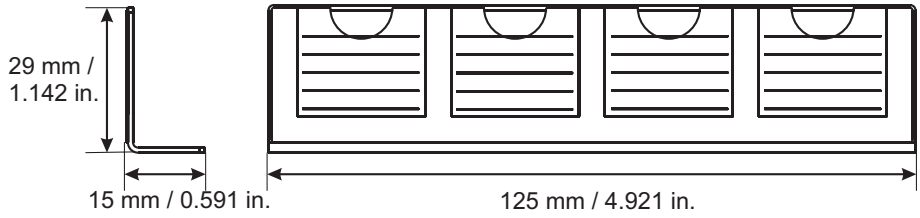


Figure 2-12 Dimensions of the labeling field

2.5 Installing the Modular Managed Switch System

2.5.1 Connecting the Supply Voltage to the FL SWITCH MM HS Head Station

24 V DC

The system is operated using a 24 V DC voltage, which is applied at the head station. If required, the voltage can also be supplied redundantly (see Figure 2-14).

If redundant power supply monitoring is active (default setting), an error is indicated if only one voltage is applied. A bridge between US1 and US2 (dotted line connection) prevents this error message. It is also possible to deactivate monitoring in web-based management or via SNMP.

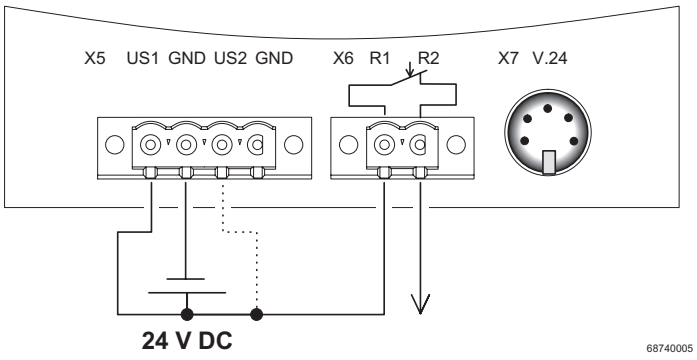


Figure 2-13 Supplying the system using one voltage source

Redundant 24 V DC supply

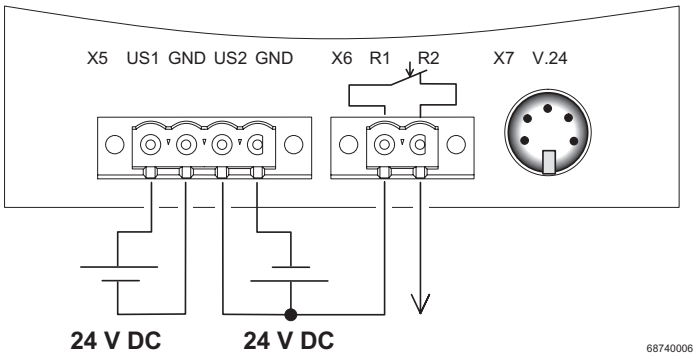


Figure 2-14 Supplying the system using two voltage sources

2.5.2 Connecting the Supply Voltage to the FL SWITCH MM HS/M for GL-Certified Operation

For GL-certified operation, an NEF 1- 3 filter (for Environmental Category EMC2) or NEF 1- 6 (for EMC1) must be used and the components must be installed in a metal control cabinet.

24 V DC

The system is operated using a 24 V DC voltage, which is applied at the head station. If required, the voltage can also be supplied redundantly (see Figure 2-16).

If redundant power supply monitoring is active (default setting), an error is indicated if only one voltage is applied. A bridge between US1 and US2 (dotted line connection) prevents this error message. It is also possible to deactivate monitoring in web-based management or via SNMP.

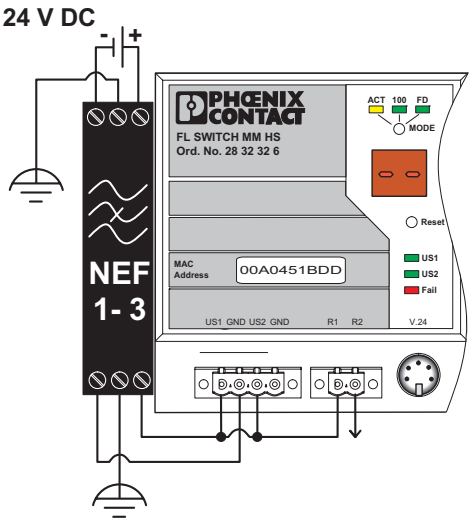


Figure 2-15 Supplying the system using one voltage source

Redundant 24 V DC supply

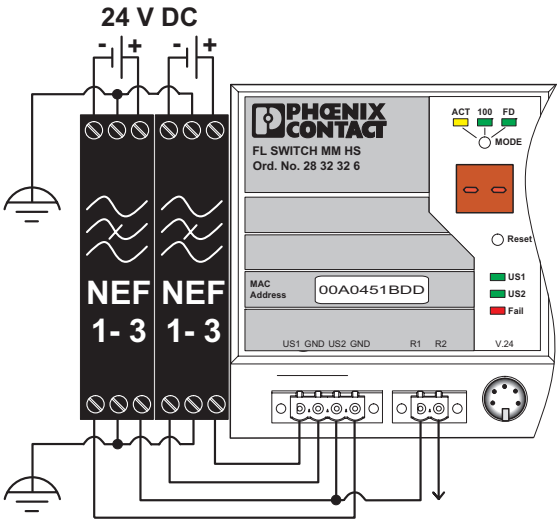


Figure 2-16 Supplying the system using two voltage sources

2.5.3 Alarm Contact

The switch has a floating alarm contact. An error is indicated when the contact is opened.

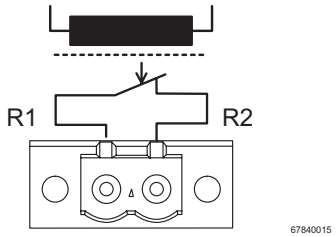


Figure 2-17 Circuit diagram for the alarm contact

The indicated error states are configured in web-based management or via SNMP. For a list of error states that can be configured, please refer to "Diagnostics/Alarm Contact" Menu on page 4-36.

In the event of non-redundant power supply, the switch indicates a supply voltage failure by opening the alarm contact. This error message can be prevented by connecting the supply voltage to both terminals in parallel, as shown in Figure 2-13 or Figure 2-15 (for GL), or by deactivating redundant power supply monitoring in web-based management.

2.5.4 V.24 (RS-232) Interface for External Management

The 6-pos. Mini-DIN female connector provides a serial interface to connect a local management station. It can be used to connect a VT100 terminal or a PC with corresponding terminal emulation to the management interface (for an appropriate cable, please refer to page 11-6). Set the following transmission parameters:

Bits per second	38400
Data bits	8
Parity	None
Stop bits	1
Flow control	None

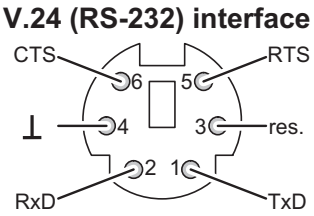


Figure 2-18 Transmission parameters and assignment of the V.24 (RS-232) interface

2.6 Grounding

Grounding protects people and machines against hazardous voltages. To avoid these dangers, correct installation, taking the local conditions into account, is vital.

All Factory Line devices must be grounded so that any possible interference is shielded from the data telegram and discharged to ground potential.

A wire of at least 2.5 mm^2 must be used for grounding. When mounting on a DIN rail, the DIN rail must be connected with protective earth ground using grounding terminal blocks. The module is connected to protective earth ground via the metal header.

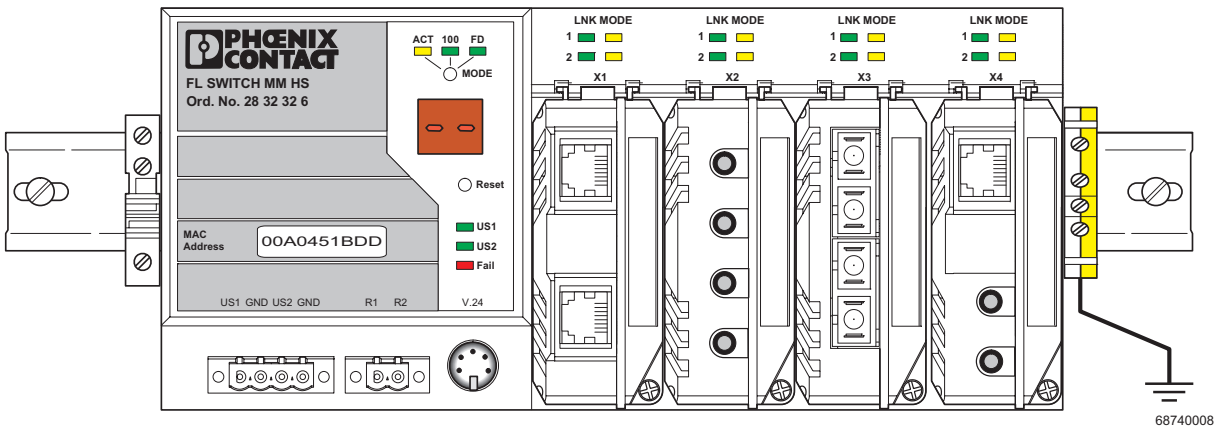


Figure 2-19 Switch on a grounded DIN rail

3 Startup and Functions

3.1 Basic Settings

The basic Ethernet functions do not have to be configured and are available when the supply voltage is switched on.

3.1.1 Default Upon Delivery/Default Settings

By default upon delivery or after the system is reset to the default settings, the following functions and properties are available:

– The password is "private".
– All IP parameters are deleted. The switch has **no** valid IP parameters:
  IP address: 0.0.0.0
  Subnet mask: 0.0.0.0
  Gateway: 0.0.0.0
– BootP is activated as the addressing mechanism.
– All available ports are activated with the following parameters:
  - Auto negotiation.
  - 100 Mbps - full duplex for FX glass fiber modules and HCS ports.
– All counters of the SNMP agent are deleted.
– The web and Telnet server, SNMP agent, and V.24 (RS-232) interface are active.
– Port mirroring, Rapid Spanning Tree, access control for web interface, port security, multicast filtering, VLAN, DHCP relay agent option 82, and LLDP are deactivated.
– Port security is deactivated for all ports.
– Access control for WBM is deactivated.
– The alarm contact only opens in the event of non-redundant power supply and a detected PoE error.
– The transmission of SNMP traps is deactivated and the switch has no valid trap destination IP address.
– The aging time is set to 40 seconds.
– The switch is in "Default" mode.
– The WBM refresh interval is set to 30 seconds.
– Management is in VLAN 1.

The aging time is set using the "dot1dTpAgingTime" MIB object (OID 1.3.6.1.2.1.17.4.2). The available setting range is 10 - 825 seconds. For static configuration, an aging time of 300 seconds is recommended.

During switch restart, the active configuration including IP parameters is written to a plugged-in memory module.

3.1.2 Assigning IP Parameters

When the supply voltage is switched on or the reset button is pressed, the switch sends requests (BootP requests) to assign IP parameters.

The button must be held down for a few seconds to trigger a reset.

The "BootP" function can be deactivated via the management. By default upon delivery, the "BootP" function is activated.

The assignment of valid IP parameters is vital to the management function of the switch.

If the switch has not received any valid IP parameters, "01" or "dc" appears in the display and one of the mode LEDs (ACT, 100 or FD) flashes.

Options for Assigning IP Parameters:

– Configuration via the BootP protocol (default upon delivery)
– Static configuration via the management interfaces
– DHCP (Dynamic Host Configuration Protocol)
– DCP (Discovery and Configuration Protocol)

4.1.2 on page 4-1 describes the assignment of IP parameters with Factory Manager 2.1.

3.1.2.1 Valid IP Parameters

IP parameters comprise the following three elements: "IP address", "subnet mask", and "default gateway/router".

Valid IP addresses are:
000.000.000.001 to 126.255.255.255
128.000.000.000 to 223.255.255.255

Valid multicast addresses are:
224.000.000.001 to 239.255.255.255

Valid subnet masks are:
255.000.000.000 to 255.255.255.252

Default gateway/router:
The IP address of the gateway/router must be in the same subnetwork as the address of the switch.

3.1.2.2 Assigning IP Addresses

The IP address is a 32-bit address, which consists of a network part and a user part. The network part consists of the network class and the network address.
There are currently five defined network classes; Classes A, B, and C are used in modern applications, while Classes D and E are hardly ever used. It is therefore usually sufficient if a network device only "recognizes" Classes A, B, and C.

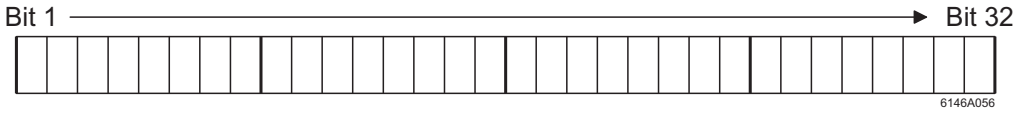


Figure 3-1 Position of bits within the IP address

With binary representation of the IP address the network class is represented by the first bits. The key factor is the number of "ones" before the first "zero". The assignment of classes is shown in the following table. The empty cells in the table are not relevant to the network class and are already used for the network address.

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5
Class A	0				
Class B	1	0			
Class C	1	1	0		
Class D	1	1	1	0	
Class E	1	1	1	1	0

The bits for the network class are followed by those for the network address and the user address. Depending on the network class, a different number of bits are available, both for the network address (network ID) and the user address (host ID).

	Network ID	Host ID
Class A	7 bits	24 bits
Class B	14 bits	16 bits
Class C	21 bits	8 bits
Class D	28-bit multicast identifier	
Class E	27 bits (reserved)	

IP addresses can be represented in decimal or hexadecimal form. In decimal notation, bytes are separated by dots (dotted decimal notation) to show the logical grouping of the individual bytes.

The decimal points do not divide the address into a network and user address. Only the value of the first bits (before the first "zero") specifies the network class and the number of remaining bits in the address.

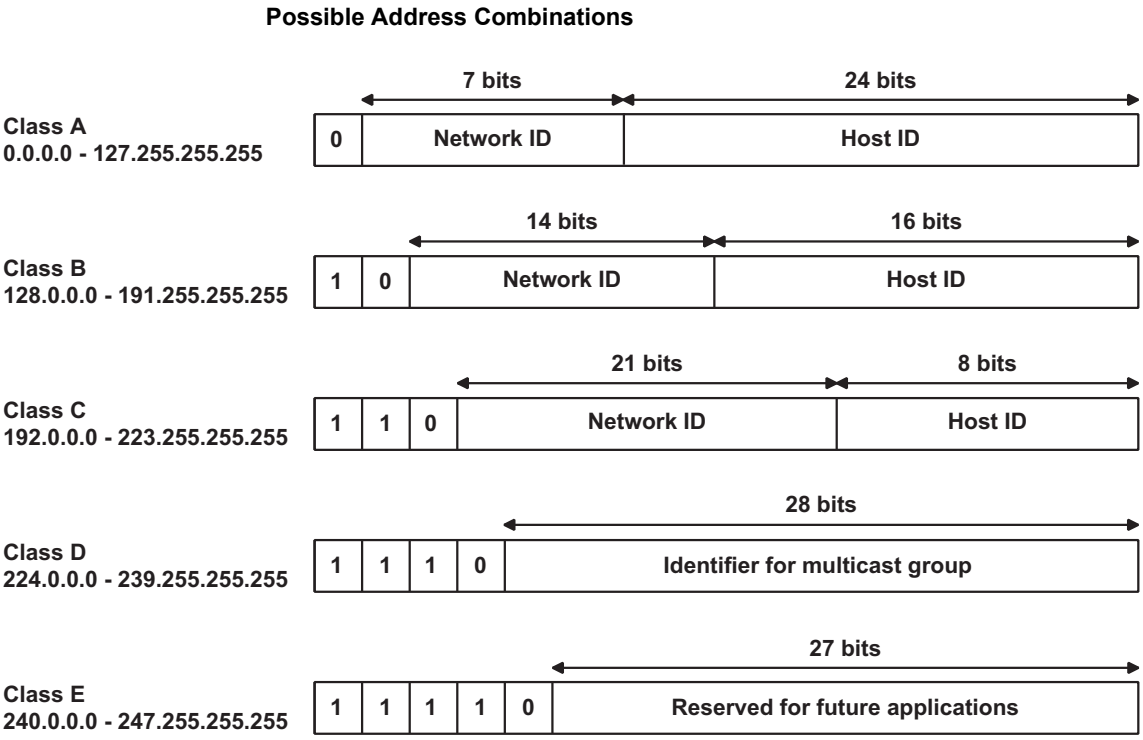


Figure 3-2 Structure of IP addresses

3.1.2.3 Special IP Addresses for Special Applications

Certain IP addresses are reserved for special functions. The following addresses should not be used as standard IP addresses.

127.x.x.x Addresses

The Class A network address "127" is reserved for a loopback function on all computers, regardless of the network class. This loopback function may only be used on networked computers for internal test purposes.

If a telegram is addressed to a computer with the value 127 in the first byte, the receiver immediately sends the telegram back to the transmitter.

The correct installation and configuration of the TCP/IP software, for example, can be checked in this way.

As Layers 1 and 2 of the ISO/OSI reference model are not included in the test they should be tested separately using the ping function.

Value 255 in the Byte

Value 255 is defined as a broadcast address. The telegram is sent to all the computers that are in the same part of the network. Examples: 004.255.255.255, 198.2.7.255 or 255.255.255.255 (all the computers in all the networks). If the network is divided into subnetworks, the subnet masks must be observed during calculation, otherwise some devices may be omitted. Simplified: The last address of an area is reserved as the broadcast address.

0.x.x.x Addresses

Value 0 is the ID of the specific network. If the IP address starts with a zero, the receiver is in the same network. Example: 0.2.1.1 refers to device 2.1.1 in this network.

The zero previously signified the broadcast address. If older devices are used, unauthorized broadcast and complete overload of the entire network (broadcast storm) may occur when using the IP address 0.x.x.x.

3.1.2.4 Subnet Masks

Routers and gateways divide large networks into several subnetworks. The IP addresses for individual devices are assigned to specific subnetworks by the subnet mask. The **network part** of an IP address is **not** modified by the subnet mask. An extended IP address is generated from the user address and subnet mask. Because the masked subnetwork is only recognized by the local computers, this extended IP address appears as a standard IP address to all the other devices.

Structure of the Subnet Mask

The subnet mask always contains the same number of bits as an IP address. The subnet mask has the same number of bits (in the same position) set to "one", which is reflected in the IP address for the network class.

Example: An IP address from Class A contains a 1-byte network address and a 3-byte computer address. Therefore, the first byte of the subnet mask may only contain "ones".

The remaining bits (three bytes) then contain the address of the subnetwork and the computer. The extended IP address is created when the bits of the IP address and the bits of the subnet mask are ANDed. Because the subnetwork is only recognized by local devices, the corresponding IP address appears as a "normal" IP address to all the other devices.

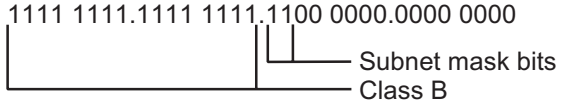
Application

If the ANDing of the address bits gives the local network address and the local subnetwork address, the device is located in the local network. If the ANDing gives a different result, the data telegram is sent to the subnetwork router.

Example for a Class B subnet mask:

Decimal notation: 255.255.192.0

Binary notation: 1111 1111.1111 1111.1100 0000.0000 0000



Using this subnet mask, the TCP/IP protocol software differentiates between the devices that are connected to the local subnetwork and the devices that are located in other subnetworks.

Example: Device 1 wants to establish a connection with device 2 using the above subnet mask. Device 2 has IP address 59.EA.55.32.

IP address display for device 2:

Hexadecimal notation:	59.EA.55.32
Binary notation:	0101 1001.1110 1010.0101 0101.0011 0010

The individual subnet mask and the IP address for device 2 are then ANDed bit-by-bit by the software to determine whether device 2 is located in the local subnetwork.

ANDing the subnet mask and IP address for device 2:

Subnet mask:	1111 1111.1111 1111.1100 0000.0000 0000
	AND
IP address:	0101 1001.1110 1010.0101 0101.0011 0010
Result after ANDing:	0101 1001.1110 1010.0100 0000.0000 0000

Sub network

After ANDing, the software determines that the relevant subnetwork (01) does not correspond to the local subnetwork (11) and the data telegram is forwarded to a subnetwork router.

3.1.3 Flowchart After a Restart

3.1.3.1 Loading the configuration data

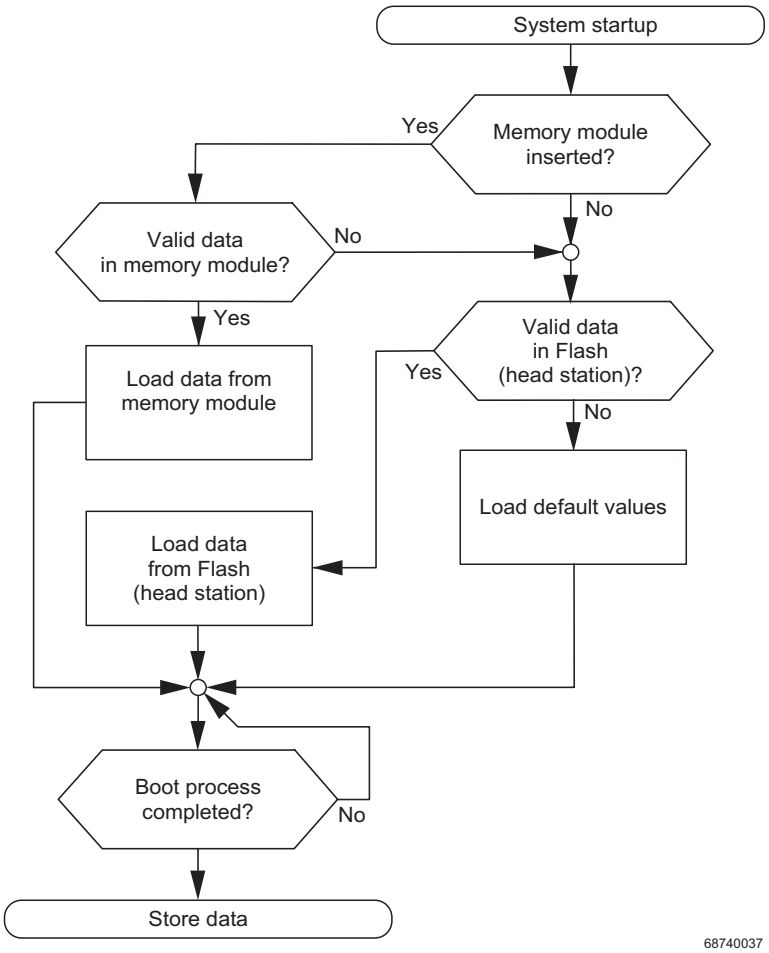


Figure 3-3 Flowchart: Loading the configuration data

3.1.3.2 Assigning IP Parameters

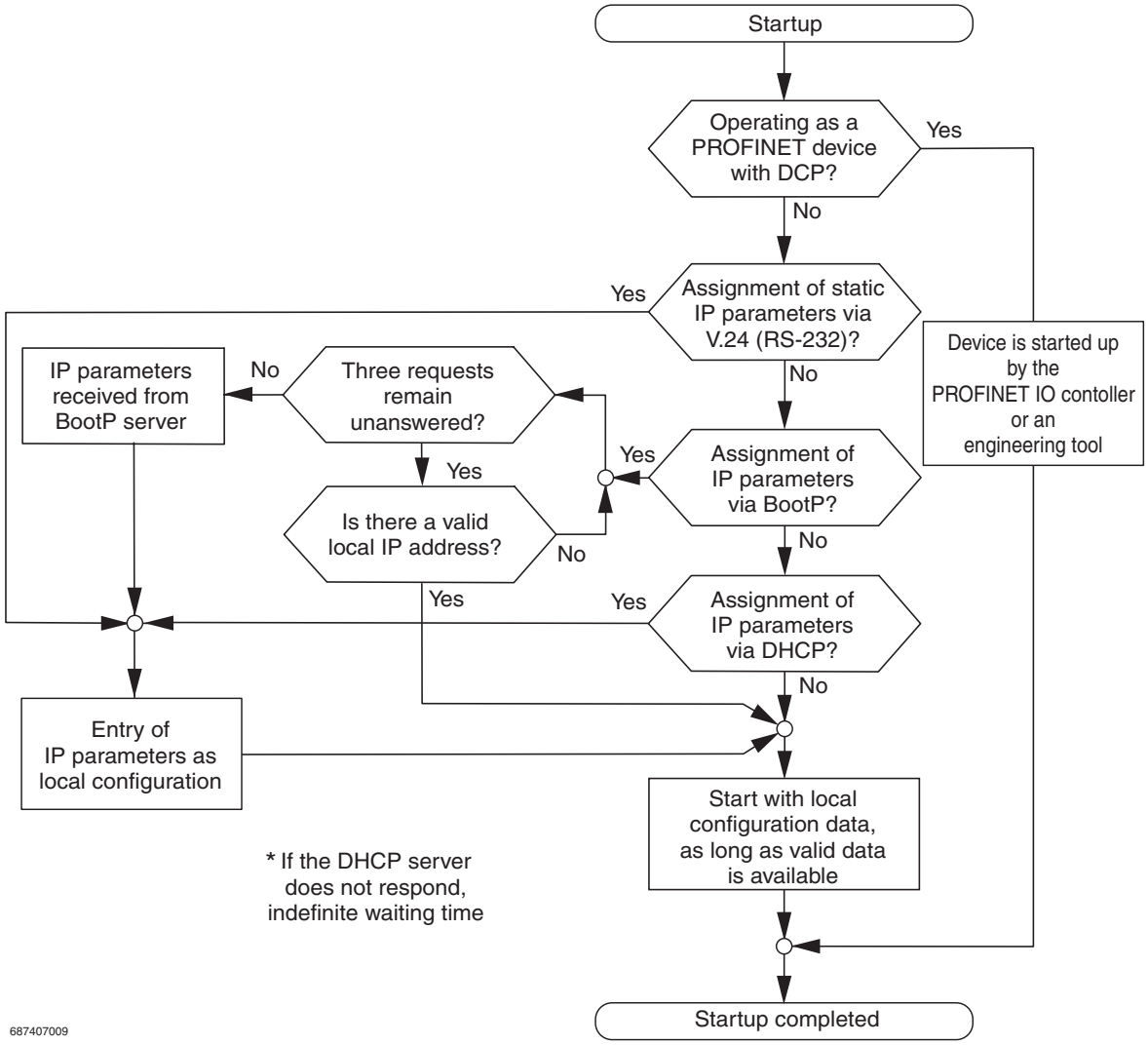

Startup
Operating as a PROFINET device with DCP?
Yes
No
Assignment of static IP parameters via V.24 (RS-232)?
Yes
No
Device is started up by the PROFINET IO contoller or an engineering tool
IP parameters received from BootP server
No
Three requests remain unanswered?
Yes
Is there a valid local IP address?
No
Yes
Assignment of IP parameters via BootP?
Yes
No
Assignment of IP parameters via DHCP?
Yes
No
Entry of IP parameters as local configuration
Start with local configuration data, as long as valid data is available
* If the DHCP server does not respond, indefinite waiting time
Startup completed
687407009

Figure 3-4 Flowchart: Assigning IP parameters

If DHCP is selected as the assignment mechanism, the DHCP server must offer a DHCP lease time of **at least five** minutes, so that the switch accepts the assigned IP parameters.

3.2 Starting Up Interface Modules

For GL-certified operation, only the interface modules listed in the table below are permitted.

Table 3-1 Interface modules with GL approval

Designation	Order No.
FL IF MEM 2TX-D	2832483
FL IF 2FX SC-D	2832425
FL IF 2FX SM SC-D	2832205
FL IF 2TX VS-RJ-F	2832344
FL IF 2TX VS-RJ-D	2832357

3.2.1 FL IF 2TX VS-RJ ...

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

3.2.1.1 Default Upon Delivery

When the interface modules are inserted, the auto negotiation and auto crossing functions are activated. Link monitoring for the twisted pair ports is not activated.

If an interface module is inserted in an MMS that has already been parameterized, the existing configuration remains active.

3.2.1.2 Functions

– Auto negotiation
  Auto negotiation is a method whereby the switch automatically detects the operating parameters for the connected network and sets the corresponding parameters (10 Mbps or 100 Mbps data transmission rate and half or full duplex transmission mode) for its RJ45 ports. Automatic port setting eliminates the need for manual intervention by the user. The auto negotiation function can be activated/deactivated via the web interface.
– Auto crossing
  There is no need to distinguish between 1:1 and crossover cables, as the transmit and receive cables are crossed automatically.

Auto crossing is only available if auto negotiation is activated.

– Auto polarity
  The polarity is changed automatically by the switch if a pair of twisted pair receive cables (RD+ and RD-) are connected incorrectly.

– Line monitoring
  The switch uses link test pulses according to standard IEEE 802.3 at regular intervals to monitor the connected TP/TX cable segments for short circuits and interrupts.

Ports that are not being used are considered cable interrupts. In addition, a TP/TX path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

3.2.1.3 Connecting the RJ45 Connectors

Insert the RJ45 male connector into the female connector according to the keying until it snaps into place. To remove the connector, press the snap-in device in the direction of the connector (A) and then remove the connector.

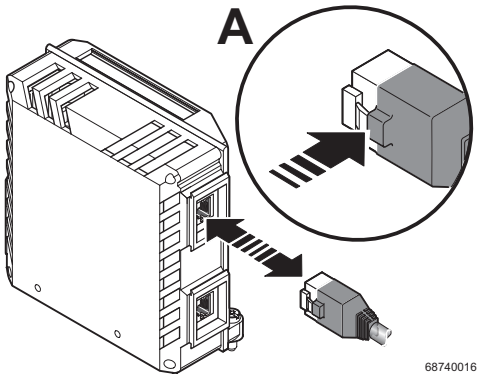


Figure 3-5 Connecting the RJ45 connectors

Industrial RJ45 Connector With Additional Latching

The figure below shows the VS-08-T-G-RJ45/IP20, which can be snapped directly onto the interface module.

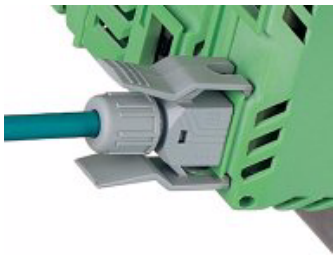


Figure 3-6 Using the VS-08-T-G-RJ45/IP20

3.2.1.4 Assignment of the RJ45 Female Connector (TP/TX)

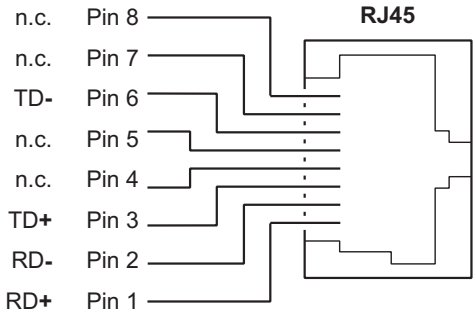


Figure 3-7 Assignment of the RJ45 female connector

3.2.2 FL IF 2POF 10/100 ...

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

3.2.2.1 Default Upon Delivery

When the interface modules are inserted, the auto negotiation function is activated, but link monitoring for the POF ports is not activated.

If an interface module is inserted in an MMS that has already been parameterized, the existing configuration remains active.

3.2.2.2 Functions

– Line monitoring
  According to standard IEEE 802.3, the switch monitors the connected fiber optic cables for interrupts.

Ports that are not being used are considered cable interrupts. In addition, a POF path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

– Auto negotiation
  Auto negotiation is a method whereby the switch automatically detects the operating parameters for the connected network and sets the corresponding parameters (10 Mbps/100 Mbps data transmission rate and half/full duplex transmission mode) for its F-SMA ports. Automatic port setting eliminates the need for manual intervention by the user. The auto negotiation function can be activated/deactivated via the web interface.

3.2.2.3 Connecting the F-SMA Connectors

To prevent dirt from entering the connectors, do not remove the dust protection caps until just before connecting the connectors. The same applies for the protective caps on the connectors.

F-SMA is a standardized fiber optic connection. We recommend the use of easy to operate F-SMA connectors with quick mounting connection from Phoenix Contact.
The connectors are secured on the interface module by manually tightening the screw collar.

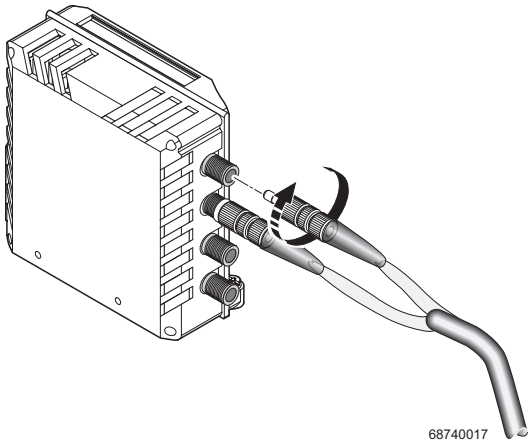


Figure 3-8 Connecting the F-SMA connectors

3.2.2.4 POF Connection Between Devices

When connecting two POF interface modules, note the signal direction of the fiber optics. The fiber connection is always from the transmitter to the receiver.

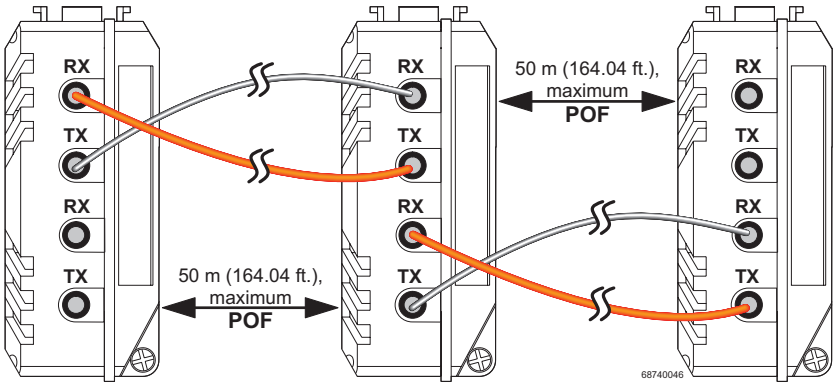


Figure 3-9 POF connection

3.2.2.5 Reducing the Transmission Power

In polymer fiber optic paths (POF) < 20 m, the transmission power must be reduced. Slide the switch on the top of the interface module to the "OFF" position. Note the assignment of port numbers.

The switch position can be read in WBM or via SNMP.

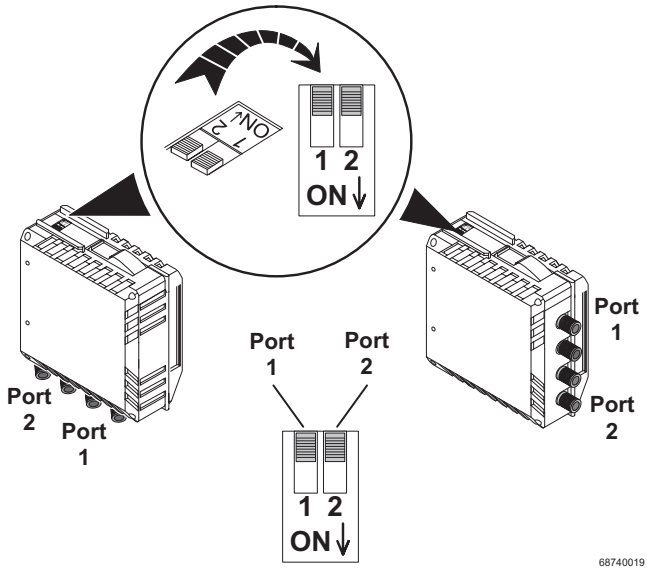


Figure 3-10 Assignment of F-SMA ports to the DIP switch

3.2.3 FL IF 2HCS 100 ...

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

3.2.3.1 Default Upon Delivery

When the interface modules are inserted, the link monitoring function for the HCS ports is not activated.

An HCS port is set to 100 Mbps - full duplex. If an HCS port is removed, the port mode is set to auto negotiation.

3.2.3.2 Functions

– Line monitoring
  According to standard IEEE 802.3, the switch monitors the connected fiber optic cables for interrupts.

Ports that are not being used are considered cable interrupts. In addition, an HCS path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

3.2.3.3 Connecting the F-SMA Connectors

To prevent dirt from entering the connectors, do not remove the dust protection caps until just before connecting the connectors. The same applies for the protective caps on the connectors.

F-SMA is a standardized fiber optic connection. We recommend the use of easy to operate F-SMA connectors with quick mounting connection from Phoenix Contact.
The connectors are secured on the interface module by manually tightening the screw collar.

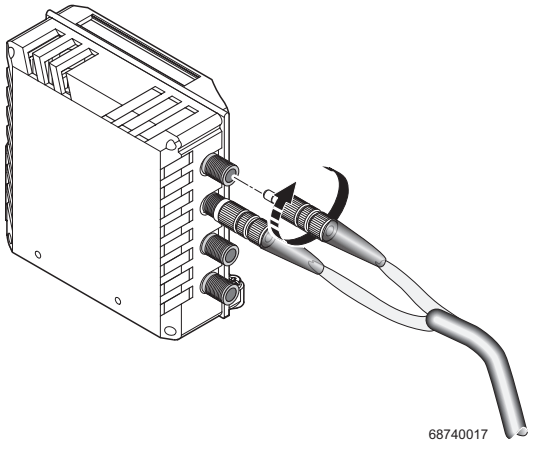


Figure 3-11 Connecting the F-SMA connectors

3.2.3.4 HCS Connection Between Devices

When connecting two HCS interface modules, note the signal direction of the fiber optics. The fiber connection is always from the transmitter to the receiver.

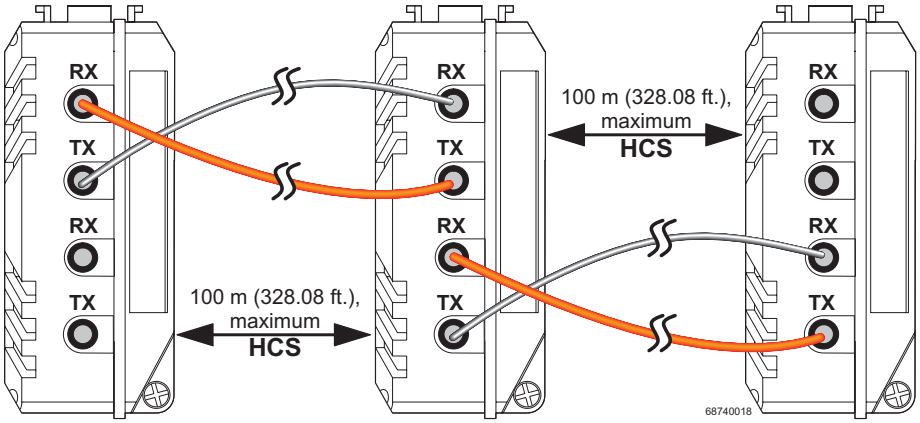


Figure 3-12 HCS connection

3.2.4 FL IF 2FX SC .../FL IF 2FX SM SC ...

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

If the FL IF 2FX (SM) SC... interface is removed and another interface type is inserted in its place, the ports are set to auto negotiation.

3.2.4.1 Default Upon Delivery

When the interface modules are inserted, they are preset with a data transmission rate of 100 Mbps and full duplex mode, and link monitoring is not activated for the fiber optic ports.

If a fiber optic interface module is inserted in an MMS that has already been parameterized, the existing configuration remains active.

– The data transmission rate is set to 100 Mbps
– The duplex method is set to full duplex

If the module is removed, auto negotiation is enabled.

3.2.4.2 Functions

– Line monitoring
  According to standard IEEE 802.3, the switch monitors the connected fiber optic cables for interrupts.

Ports that are not being used are considered cable interrupts. In addition, a fiber optic path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

– Far End Fault Detection indicates that the connection in the direction of the partner is not OK (the partner does not indicate a link) and therefore at least one fiber within the fiber optic cable is faulty or has not been assembled correctly.

3.2.4.3 Connecting the SC-D Connectors

To prevent dirt from entering the connectors, do not remove the dust protection caps until just before connecting the connectors. The same applies for the protective caps on the connectors.

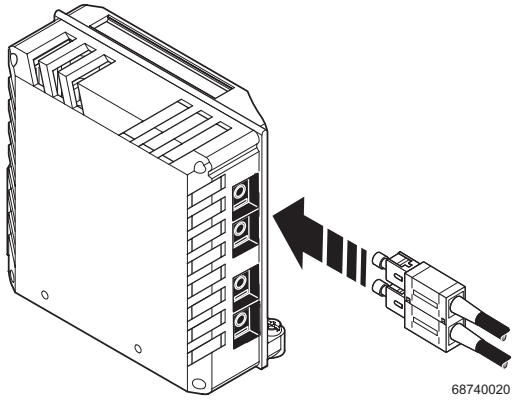


Figure 3-13 Connecting the SC-D connectors

3.2.4.4 Fiber Optic Connection Between Devices

When connecting two fiber optic interface modules, note the signal direction of the fiber optics. The fiber connection is always from the transmitter to the receiver. The SC-D/SCRJ connectors, which are connected using a support, are keyed to ensure that the assignment of the transmit and receive direction is correct.

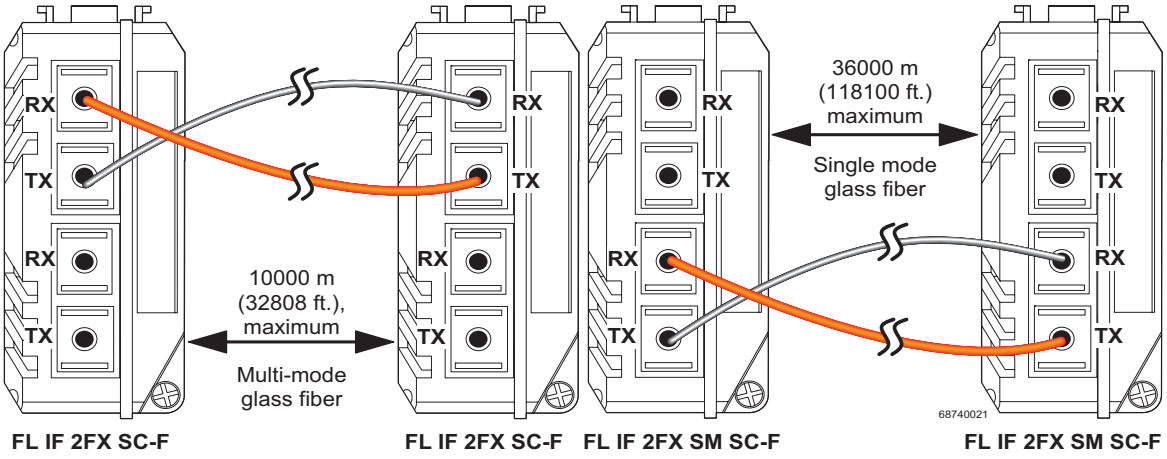


Figure 3-14 Fiber optic connection between devices

The maximum length of the fiber optic cables depends on the interface module/fiber type used.

3.2.5 FL IF 2FX ST-D

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

If the FL IF 2FX ST-D interface is removed and another interface type is inserted in its place, the ports are set to auto negotiation.

3.2.5.1 Default Upon Delivery

When the interface modules are inserted, they are preset with a data transmission rate of 100 Mbps and full duplex mode, and link monitoring is not activated for the glass fiber ports.

If a glass fiber interface module is inserted in an MMS that has already been parameterized, the existing configuration remains active.

– The data transmission rate is set to 100 Mbps
– The duplex method is set to full duplex

If the module is removed, auto negotiation is enabled.

3.2.5.2 Functions

– Line monitoring
  According to standard IEEE 802.3, the switch monitors the connected fiber optic cables for interrupts.

Ports that are not being used are considered cable interrupts. In addition, a glass fiber path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

– Far End Fault Detection indicates that the connection in the direction of the partner is not OK (the partner does not indicate a link) and therefore at least one fiber within the glass fiber cable is faulty or has not been assembled correctly.

3.2.5.3 Connecting the ST Connectors

To prevent dirt from entering the connectors, do not remove the dust protection caps until just before connecting the connectors. The same applies for the protective caps on the connectors.

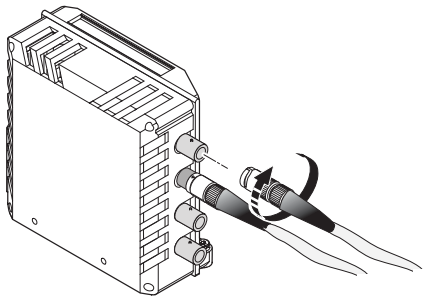


Figure 3-15 Connecting the ST connectors

3.2.5.4 Glass Fiber Connection Between Devices

When connecting two glass fiber interface modules, note the signal direction of the fiber optics. The fiber connection is always from the transmitter to the receiver.

The maximum length of the glass fiber cables depends on the fiber type used.

3.2.6 FL IF TX/POF 10/100 ...

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

3.2.6.1 Default Upon Delivery

When the interface modules are inserted, the auto negotiation and auto crossing functions are activated for the twisted pair port, and the auto negotiation function is activated for the POF port. Port monitoring is not activated for the two ports.

If an interface module is inserted in an MMS that has already been parameterized, the existing configuration remains active.

3.2.6.2 Functions of the POF Interface

– Line monitoring
  According to standard IEEE 802.3, the switch monitors the connected fiber optic cables for interrupts.

Ports that are not being used are considered cable interrupts. In addition, a POF path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

– Auto negotiation
  Auto negotiation is a method whereby the switch automatically detects the operating parameters for the connected network and sets the corresponding parameters (10 Mbps/100 Mbps data transmission rate and half/full duplex transmission mode) for its F-SMA ports. Automatic port setting eliminates the need for manual intervention by the user. The auto negotiation function can be activated/deactivated via the web interface.

3.2.6.3 Functions of the Twisted Pair Interface

– Auto negotiation
  Auto negotiation is a method whereby the switch automatically detects the operating parameters for the connected network and sets the corresponding parameters (10 Mbps/100 Mbps data transmission rate and half/full duplex transmission mode) for its RJ45 ports. Automatic port setting eliminates the need for manual intervention by the user. The auto negotiation function can be activated/deactivated via the web interface.
– Auto crossing
  There is no need to distinguish between 1:1 and crossover cables, as the transmit and receive cables are crossed automatically.

Auto crossing is only available if auto negotiation is activated.

– Auto polarity
  The polarity is changed automatically by the switch if a pair of twisted pair receive cables (RD+ and RD-) are connected incorrectly.
– Line monitoring
  The switch uses link test pulses according to standard IEEE 802.3 at regular intervals to monitor the connected TP/TX cable segments for short circuits and interrupts.

Ports that are not being used are considered cable interrupts. In addition, a TP/TX path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

3.2.6.4 Network Connection

The switch position for transmission power reduction will only be indicated in the web interface in future hardware versions.

See "FL IF 2TX VS-RJ ..." on page 3-9 and onwards, and "FL IF 2POF 10/100 ..." on page 3-11 and onwards.

3.2.7 FL IF TX/HCS 100 ...

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

3.2.7.1 Default Upon Delivery

When the interface modules are inserted, the auto negotiation and auto crossing functions are activated for the twisted pair port, and the data transmission rate is set to 100 Mbps full duplex for the HCS port. Port monitoring is not activated for the two ports.

If an interface module is inserted in an MMS that has already been parameterized, the existing configuration remains active.

3.2.7.2 Functions of the HCS Interface

– Line monitoring
  According to standard IEEE 802.3, the switch monitors the connected fiber optic cables for interrupts.

Ports that are not being used are considered cable interrupts. In addition, an HCS path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

3.2.7.3 Functions of the Twisted Pair Interface

– Auto negotiation
  Auto negotiation is a method whereby the switch automatically detects the operating parameters for the connected network and sets the corresponding parameters (10 Mbps/100 Mbps data transmission rate and half/full duplex transmission mode) for its RJ45 ports. Automatic port setting eliminates the need for manual intervention by the user. The auto negotiation function can be activated/deactivated via the web interface.
– Auto crossing
  There is no need to distinguish between 1:1 and crossover cables, as the transmit and receive cables are crossed automatically.

Auto crossing is only available if auto negotiation is activated.

– Auto polarity
  The polarity is changed automatically by the switch if a pair of twisted pair receive cables (RD+ and RD-) are connected incorrectly.
– Line monitoring
  The switch uses link test pulses according to standard IEEE 802.3 at regular intervals to monitor the connected TP/TX cable segments for short circuits and interrupts.

Ports that are not being used are considered cable interrupts. In addition, a TP/TX path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

3.2.7.4 Network Connection

See "FL IF 2TX VS-RJ ..." on page 3-9 and onwards, and "FL IF 2HCS 100 ..." on page 3-14 and onwards.

3.2.8 FL IF MEM 2TX-D

Make sure that only one memory module is inserted. If more than one module is inserted, the switch indicates error code "87" on the display. Remove all but one of the memory modules and restart the switch.

The interface module has two twisted pair interfaces in addition to the parameterization memory. To distinguish it from other 2TX interface modules, it is supplied in charcoal-gray housing. The parameterization memory is used to store device data, which is modified by the user and stored retentively.

The memory module is supported by firmware Version 2.03 or later. Firmware Versions < 2.03 treat the memory module as a "standard" FL IF 2TX VS-RJ.

The use of memory modules requires the application of system bus firmware 4.20 or later in the head station. The system bus firmware for your head station is displayed on the "Device Information/General" web page.

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

If the module is removed when saving, the configuration is not saved. The saving procedure is finished as soon as the display **no** longer indicates "SC" or when the status "Current Configuration was saved" is indicated on the **"Configuration Management"** web page.

3.2.8.1 Parameterization Memory Default Upon Delivery

By default upon delivery, the parameterization memory is empty (see "Default Upon Delivery/Default Settings" on page 3-1).

3.2.8.2 Twisted Pair Interface Default Upon Delivery

When the interface modules are inserted, the auto negotiation and auto crossing functions are activated. Link monitoring for the twisted pair ports is not activated.

If an interface module is inserted in an MMS that has already been parameterized, the existing configuration remains active.

3.2.8.3 Function of the Memory Module

– When saving data to the Flash memory of the device, the data is also transmitted to a plugged-in memory module.

If the user resets the module to the settings default upon delivery, the configuration is also saved on the memory module. See "Default Upon Delivery/Default Settings" on page 3-1.

– Data is stored to the Flash memory of the head station and in the memory module:
  - After a system startup
  - On request by the user

– When starting the MMS, the data is read from a plugged-in memory module (display indicates "OP") and used as the active configuration. The data in the Flash memory is overwritten by the data from the memory module.

Please note that the password stored on the memory module is also transmitted to the MMS. Make sure that you know the password for the configuration on the memory module.

3.2.8.4 Functions of the Twisted Pair Interface

– Auto negotiation
  Auto negotiation is a method whereby the switch automatically detects the operating parameters for the connected network and sets the corresponding parameters (10 Mbps/100 Mbps data transmission rate and half/full duplex transmission mode) for its RJ45 ports. Automatic port setting eliminates the need for manual intervention by the user. The auto negotiation function can be activated/deactivated via the web interface.
– Auto crossing
  There is no need to distinguish between 1:1 and crossover cables, as the transmit and receive cables are crossed automatically.

Auto crossing is only available if auto negotiation is activated.

– Auto polarity
  The polarity is changed automatically by the switch if a pair of twisted pair receive cables (RD+ and RD-) are connected incorrectly.
– Line monitoring
  The switch uses link test pulses according to standard IEEE 802.3 at regular intervals to monitor the connected TP/TX cable segments for short circuits and interrupts.

Ports that are not being used are considered cable interrupts. In addition, a TP/TX path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

3.2.8.5 Network Connection

See "FL IF 2TX VS-RJ ..." on page 3-9 and onwards.

3.2.9 FL IF 2PSE-F

The PoE interface module is supported by firmware Version 4.0 or later. Firmware Versions < 4.0 treat the module as a standard RJ45 interface module. The module can operate in PoE mode without management and without support from the firmware and hardware (system bus) (see note below). No configuration options and no diagnostic data are available, connected termination devices are nevertheless supplied with power.

The use of the PoE interface module requires the application of system bus firmware 5.00 or later in the head station and system bus firmware 4.00 or later in the extension modules. If this requirement is not met in the head station or in any extension module, then PoE management is not available in the **entire** system. The system bus firmware is displayed on the "Device Information/General" web page.

PoE management and PoE information are only available if the 48 V supply is connected to the relevant PoE interface module. The ports can be used as standard RJ45 ports if there is no connected supply.

Features of PoE Mode

– Up to twelve PoE interface modules with a total of 24 ports can be operated at the same time in an MMS.
– Configuration is still possible if the interface module is not plugged in or the 48 V supply is not connected.
– PoE management and PoE information are only available if the interface module is plugged in and there is a connected 48 V supply.
– The following management functions are available:
  - Display error states for each port and communicate via the alarm contact (yes/no)
  - Connect/disconnect voltage for each port
  - Switch current limitation on or off for loads classified as Class 1 devices
– Send Traps when the PoE status changes
– The following diagnostic information is displayed:
  - No error
  - Surge voltage/undervoltage
  - Thermal error
  - Overload
  - Disconnected load (the current consumption at this port is less than 10 mA, the supply voltage is disconnected by the PoE module)
  - No 48 V supply

- No PoE interface module detected at this port
- No hardware support due to the system bus
- Detected class of a connected termination device (Class 0 to Class 4)
- Output voltage and output current

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

3.2.9.1 Default Upon Delivery

When the interface modules are inserted, the auto negotiation and auto crossing functions are activated. Link monitoring for the twisted pair ports is not activated.

If an interface module is inserted in an MMS that has already been parameterized, the existing configuration remains active.

3.2.9.2 Functions

– Auto negotiation
  Auto negotiation is a method whereby the switch automatically detects the operating parameters for the connected network and sets the corresponding parameters (10 Mbps or 100 Mbps data transmission rate and half or full duplex transmission mode) for its RJ45 ports. Automatic port setting eliminates the need for manual intervention by the user. The auto negotiation function can be activated/deactivated via the web interface.
– Auto crossing
  There is no need to distinguish between 1:1 and crossover cables, as the transmit and receive cables are crossed automatically.

Auto crossing is only available if auto negotiation is activated.

– Auto polarity
  The polarity is changed automatically by the switch if a pair of twisted pair receive cables (RD+ and RD-) are connected incorrectly.
– Line monitoring
  The switch uses link test pulses according to standard IEEE 802.3 at regular intervals to monitor the connected TP/TX cable segments for short circuits and interrupts.

Ports that are not being used are considered cable interrupts. In addition, a TP/TX path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

The PoE configuration options are also available if no PoE interface module is inserted. If a PoE interface module is inserted, the configuration is transmitted to the module after a few seconds.

3.2.9.3 Network Connection

See "FL IF 2TX VS-RJ ..." on page 3-9 and onwards.

3.2.9.4 Connecting the 48 V PoE Supply Voltage

Connecting the PoE Supply

The connector for the PoE supply is located on the bottom of the interface module. Please observe the keying on the connector when inserting it.
The module has a green LED for each port, which indicates the PoE mode. The LED is active if the PoE supply **and** a PD (powered device) are connected. The LED flashes if the module is supplied with less than 48 V.

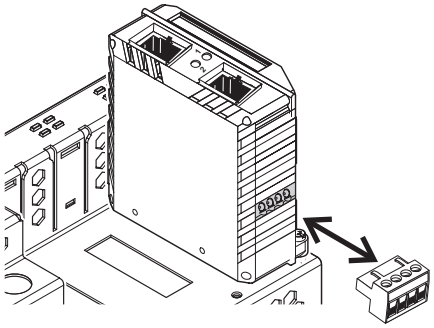


Figure 3-16 Connecting the PoE voltage connector

Connecting the PoE Supply

Connect the 48 V PoE supply to terminals 1 (+) and 2 (-). The terminals are bridged within the module. The bridges are located between terminals 1 and 3, and between terminals 2 and 4. The bridges can be used to supply voltage to a **maximum** of three additional PoE interface modules. The supply voltage to additional PoE interface modules must be supplied by power supply units.

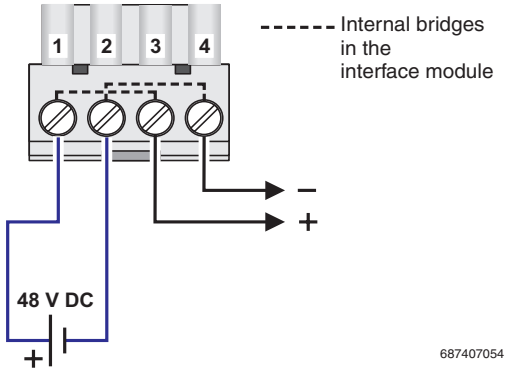


Figure 3-17 Connecting the 48 V PoE supply

Table 3-2 Pin assignment of PoE ports

Pin	Assignment	Description	Pin	Assignment	Description
1	RX+/48 V DC	Data/PoE +	5	n. c.	-
2	RX-/48 V DC	Data/PoE +	6	TX-/0 V	Data/PoE -
3	TX+/0 V	Data/PoE -	7	n. c.	-
4	n. c.	-	8	n. c.	-

3.2.10 FL IF 2POF SCRJ-D

Hot plugging
When inserting and removing interface modules, you do **not** have to switch off the supply voltage. The interface modules are detected automatically and logged to the network management.

If the FL IF 2POF SCRJ ... interface is removed and another interface type is inserted in its place, the ports are set to auto negotiation.

3.2.10.1 Default Upon Delivery

When the interface modules are inserted, they are preset with a data transmission rate of 100 Mbps and full duplex mode, and link monitoring is not activated for the fiber optic ports.

If a fiber optic interface module is inserted in an MMS that has already been parameterized, the existing configuration remains active.

– The data transmission rate is set to 100 Mbps
– The duplex method is set to full duplex

If the module is removed, auto negotiation is enabled.

3.2.10.2 Functions

– Line monitoring
  According to standard IEEE 802.3, the switch monitors the connected fiber optic cables for interrupts.

Ports that are not being used are considered cable interrupts. In addition, a fiber optic path to a deactivated termination device is also considered a cable interrupt, as the connected device cannot send a link test pulse because it is switched off.

– Far End Fault Detection indicates that the connection in the direction of the partner is not OK (the partner does not indicate a link) and therefore at least one fiber within the fiber optic cable is faulty or has not been assembled correctly.

3.2.10.3 Connecting the SCRJ Connectors

To prevent dirt from entering the connectors, do not remove the dust protection caps until just before connecting the connectors. The same applies for the protective caps on the connectors.

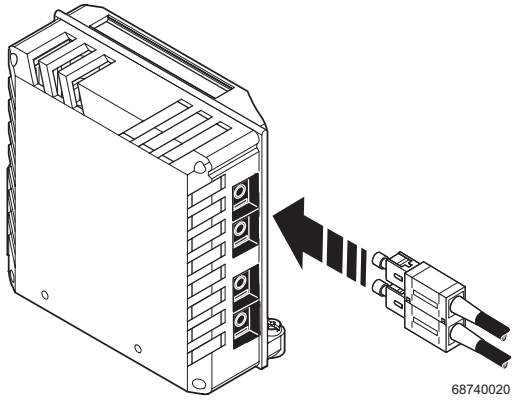


Figure 3-18 Connecting the SCRJ connectors

3.2.10.4 Fiber Optic Connection Between Devices

When connecting two fiber optic interface modules, note the signal direction of the fiber optics. The fiber connection is always from the transmitter to the receiver. The SCRJ connectors, which are connected using a support, are keyed to ensure that the assignment of the transmit and receive direction is correct.

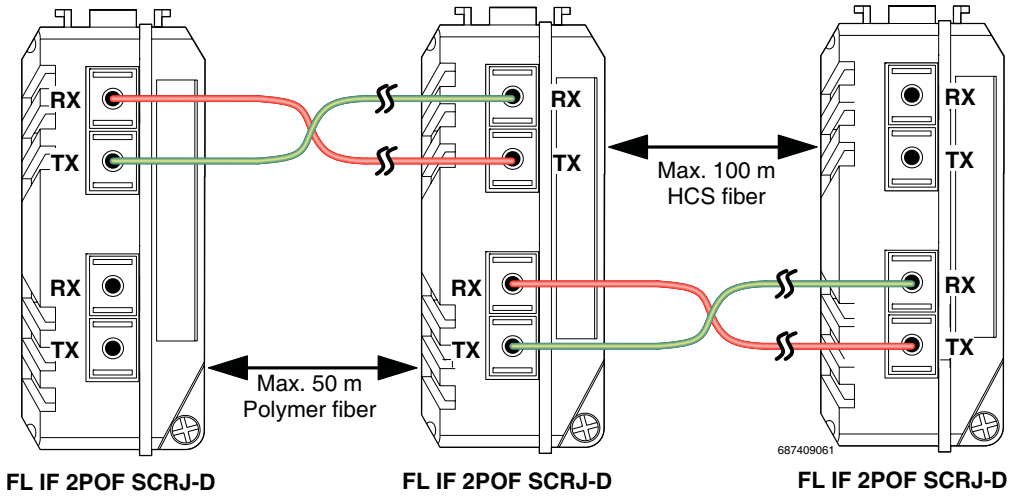


Figure 3-19 Fiber optic connection between devices

The maximum length of the fiber optic cables depends on the interface module/fiber type used.

3.2.10.5 SCRJ Modules in WBM

Very detailed information about the SCRJ modules is available in WBM (see "Ports/POF Port Table" Menu on page 4-29), e.g., the port system reserve, alarms or port states are displayed.

The following states can be displayed under "Transceiver status":

– "System Hardware does not support diagnosable POF modules" (this hardware does not support POF-SCRJ diagnostics)
– "No POF-SCRJ Interface modules present" (no POF-SCRJ module is plugged in)
– "POF-SCRJ Interface module is present and OK" (the system reserve is greater than 2 dB and is displayed under "RX system reserve")
– "POF-SCRJ Interface module is present, but the system reserve is low" (the system reserve is less than 2 dB, but greater than 0 dB)
– "POF-SCRJ Interface module is present, but the system reserve is exhausted" (no system reserve available - the received optical power is below the required minimum value)

3.3 Frame Switching

The FL SWITCH MM HS operates in store-and-forward mode. When receiving a data packet, the switch analyzes the source and destination addresses. The switch stores up to 8000 MAC addresses with an adjustable aging time of 10 to 825 seconds in its address table.

3.3.1 Store-and-Forward

All data telegrams that are received by the switch are saved and their validity is checked. Invalid or faulty data packets (> 1522 bytes or CRC errors) and fragments (< 64 bytes) are rejected. Valid data telegrams are forwarded by the switch.

3.3.2 Multi-Address Function

The switch learns all the source addresses for each port. Only packets with:

– Unknown source addresses
– A source address for this port
– A multicast/broadcast address

are forwarded to the destination address field via the relevant port. The switch can learn up to 8000 addresses. This is important when more than one termination device is connected to one or more ports. In this way, several independent subnetworks can be connected to one switch.

3.3.3 Learning Addresses

The MMS independently learns the addresses for termination devices, which are connected via a port, by evaluating the source addresses in the data telegram. When the MMS receives a data telegram, it only forwards this data telegram to the port that connects to the specified device (if the address could be learned beforehand).
The MMS can learn up to 8000 addresses and stores them in its table. The switch monitors the age of the learned addresses. The switch automatically deletes address entries from its address table that have exceeded a specific age (default: 40 seconds, adjustable from 10 to 825 seconds, aging time).

All learned entries are deleted on a restart.

A list of detected MAC addresses can be found in the MAC address table (see "Diagnostics/MAC Address Table" Menu on page 4-39). The MAC address table can be deleted via "Clear".

The aging time is set using the "dot1dTpAgingTime" MIB object (OID 1.3.6.1.2.1.17.4.2). The available setting range is 10 - 825 seconds. For static configuration, an aging time of 300 seconds is recommended.

3.3.4 Prioritization

The switch supports two priority queues for adjusting the internal packet processing sequence (traffic classes according to IEEE 802.1D). Data telegrams that are received are assigned to these classes according to their priority, which is specified in the VLAN/prioritization tag:

– Data packets with values between "0" and "3" in the priority field are low (default) priority.
– Data packets with values between "4" and "7" in the priority field are high priority and transmitted via the switch.

In addition, the switch enables port-based prioritization of data streams.

3.3.4.1 VLAN/Prioritization Tag

The MMS processes incoming data packets with regard to the prioritization information contained in the Ethernet packet (VLAN/prioritization tag).

The tag enables the specification of a priority level from 0 to 7, which the MMS assigns to one of its two internal queues. By default upon delivery, the packets with priorities from 0 to 3 are treated as low-priority packets whereas packets with priorities from 4 to 7 are high-priority Ethernet packets.

The assignment of priority levels for both internal priority levels of the MMS can be modified via the "dot1dTrafficClassTable" of the P bridge MIB.

Processing Rules

The switch controller in the MMS forwards received packets to one of the receive queues according to the following decisions:

– BPDU packets (Spanning Tree, LLDP) and IGMP packets are always assigned to the high-priority queue.
– Packets with unknown unicast addresses are always assigned to the low-priority queue.
– Packets are assigned to the high-priority queue if the priority from the VLAN/priority tag is mapped to the "high" level (default priority 4 to 7).
– The internal port priority "high" results in priority level 7 handling, i.e., the basic settings for data packet assignment to the high-priority queue are made.
– All residual data is assigned to the low-priority queue.

3.3.4.2 Port Prioritization

In addition to the processing sequence according to the priority information from the tag, the user can set the internal prioritization for every individual switch port at the MMS. In this way, the processing of Ethernet data for a particular port can be prioritized.

The port prioritizing method is suitable for termination devices that do not support tagging and thus cannot generate priorities.

"High" port prioritization sets the internal priority of the packets received at this port to priority level 7. In the switch, these packets will be processed with priority information 7 within the tag (preferred handling and forwarding method only within the MMS, however, when forwarding to the receiver, the packets are in the original state). The "Low" port prioritization means that the priority of packets received at this port is not influenced by the switch. This implies that existing tags must be taken into consideration or that other priority rules must be observed.

Setting the Port Priority

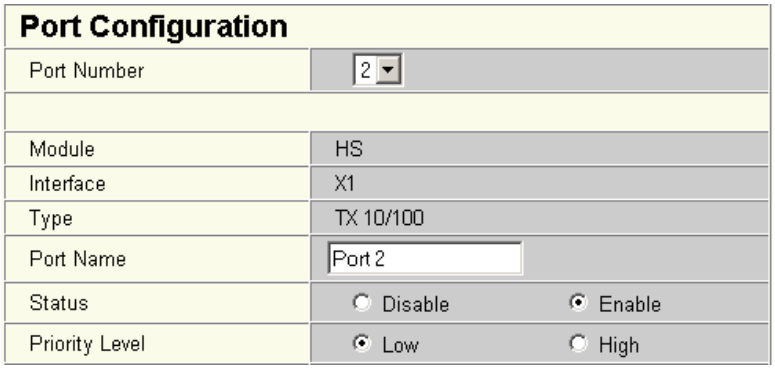


Figure 3-20 Setting the port priority

– On the "Port Configuration" web page, both available priority levels can be selected under "Priority Level".

3.3.4.3 Strict Priority

The switch supports two priority queues for adjusting the packet processing sequence (traffic classes according to IEEE 802.1D). Data telegrams that are received are assigned to these classes according to their priority, which is specified in the VLAN/prioritization tag:

– Data packets with values between "0" and "3" in the priority field are low priority (default).
– Data packets with values between "4" and "7" in the priority field are high priority and transmitted via the switch.

MMS uses "Strict Priority" for transmitting data telegrams. First, **all** high-priority data packets are assigned, once these are transmitted, low-priority telegrams are assigned.

This function prevents delays in high-priority data transmission, due to large volumes of low-priority data traffic. Low-priority traffic is rejected when the memory or data channel is overloaded.

4 Configuration and Diagnostics

The modular managed switch system offers several user interfaces for accessing configuration and diagnostic data. The preferred interfaces are the web interface and SNMP interface. These two interfaces can be used to make all the necessary settings and request all information.
Access via Telnet/V.24 (RS-232) interface only enables access to basic information. However, the V.24 (RS-232) interface also enables firmware update via XMODEM in the event of faulty firmware.

Settings are not automatically saved permanently. The active configuration can be saved permanently by selecting "Save current configuration" on the "Configuration Management" web page.

4.1 Factory Manager

4.1.1 General Function

The integration of the MMS in the Factory Manager provides optimum support for configuration and management.

4.1.2 Assigning IP Parameters

Only **one** of several options for assigning IP parameters using Factory Manager 2.2 is described here.

Once you have established all the necessary connections and Factory Manager has been started, start the MMS or execute a reset.

Following the boot phase, the MMS sends the BootP requests, which are received by the Factory Manager and displayed in the message window. If you are operating other devices in the same network, messages from these devices may also be displayed. Messages from Phoenix Contact Factory Line components can be easily identified by their MAC address, which starts with 00.A0.45... and is provided on the devices.

Please check the MAC address in the messages to ensure the correct device is addressed.

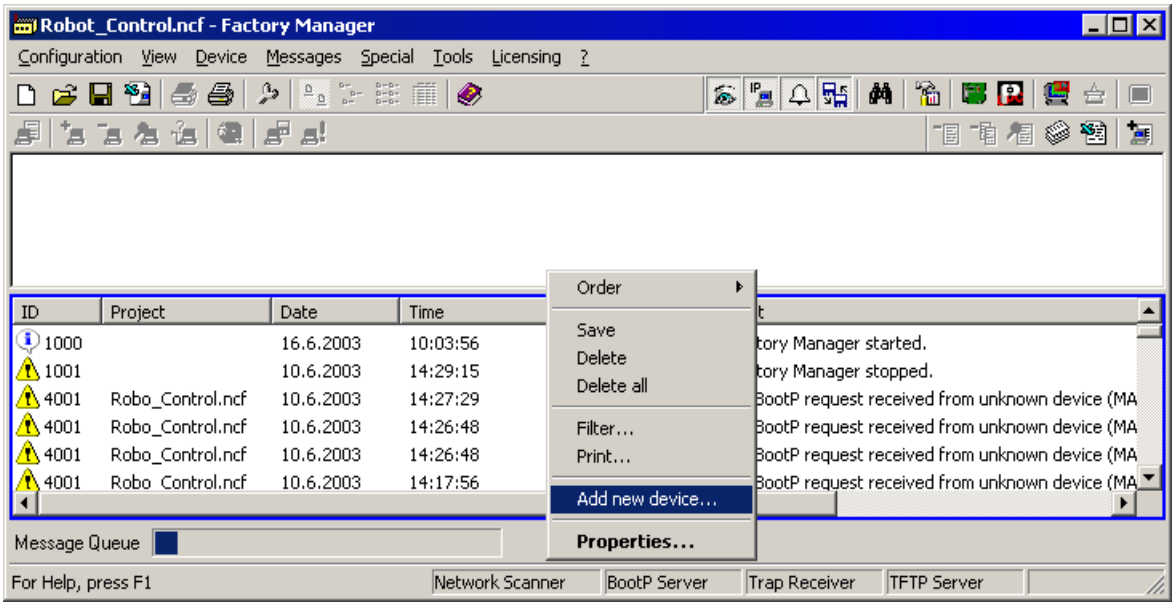


Figure 4-1 Messages from the MMS in the Factory Manager

Right-click on one of the MMS messages and select the "Add new device..." menu item. Under "Description", select an icon and enter a device name.

Specify the desired IP parameters under "TCP/IP" (see also "Assigning IP Parameters" on page 3-2).

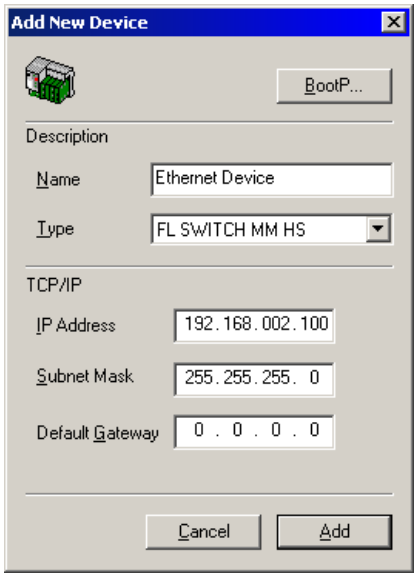


Figure 4-2 Input mask for IP parameters

Make sure that the assignment of IP parameters via BootP is also activated.

Once you have clicked on "Add", the device is added to the project and is indicated as **unavailable**. You must now restart or reset the MMS. Following a restart, the MMS resends the BootP requests and receives the corresponding BootP reply from the Factory Manager. Once the boot process has been completed the MMS is indicated as available.

If the MMS is still indicated as "unavailable", check your network card settings. Please note that both devices must be located in the same network/subnetwork. If the Factory Manager receives the BootP requests this does not mean that the devices are located in the same subnetwork, as the BootP requests are sent as a broadcast beyond subnetwork boundaries.

4.1.3 Configuration and Diagnostics

Numerous options for configuring and diagnosing the MMS can be found in the "Device" menu under "Properties".

General

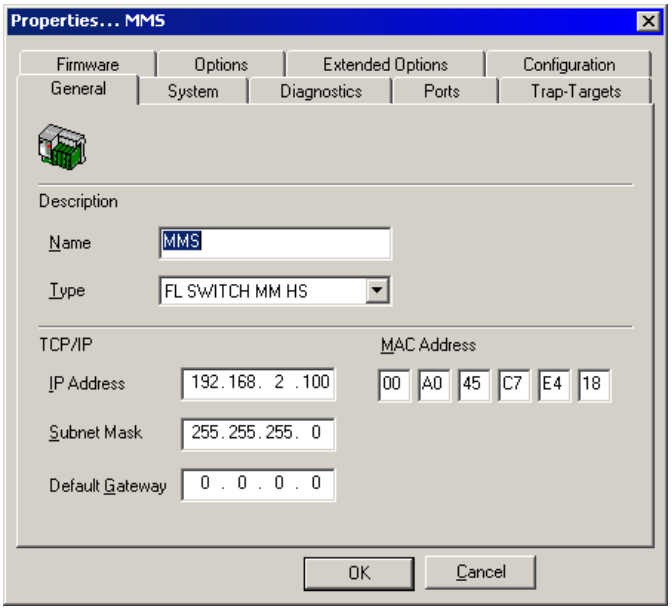


Figure 4-3 "General" menu

Here you can check or modify device names and types as well as IP parameters.

If you modify the IP address and/or the other IP parameters using the Factory Manager, once you click "OK" you will no longer have access via the Factory Manager. Restarting the MMS activates the modified parameters and restores access.

To activate the new addresses following a restart, BootP must be activated in the MMS (on the "IP Configuration" page in WBM).

System

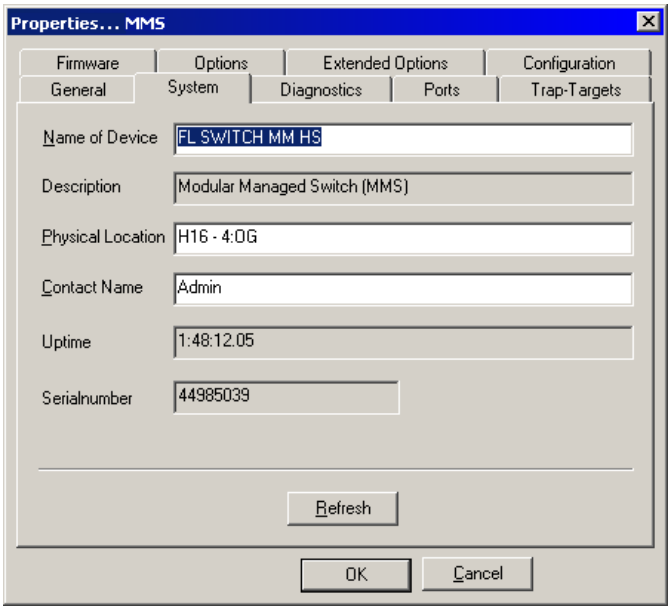


Figure 4-4 "System" menu

In this menu, you can add additional information in the white fields, which will be saved on the MMS. This information is also available via SNMP and WBM.

Diagnostics

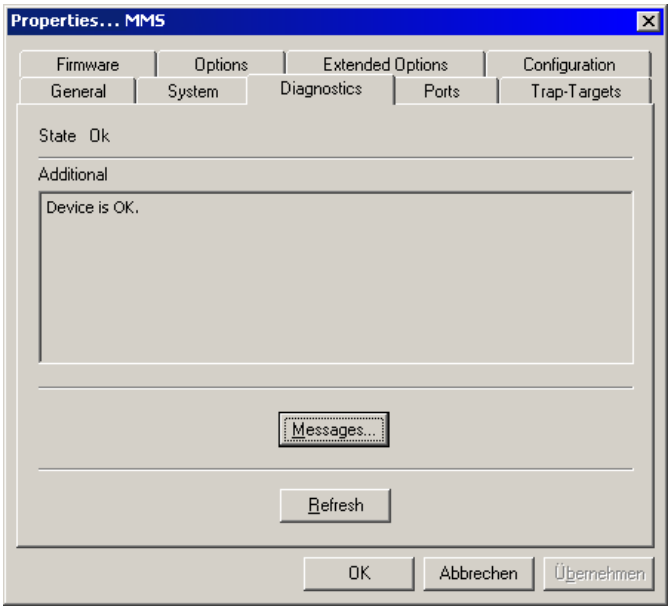


Figure 4-5 "Diagnostics" menu

Information about the device status and redundancy is displayed here. All the messages for this device are displayed under Messages.

Ports

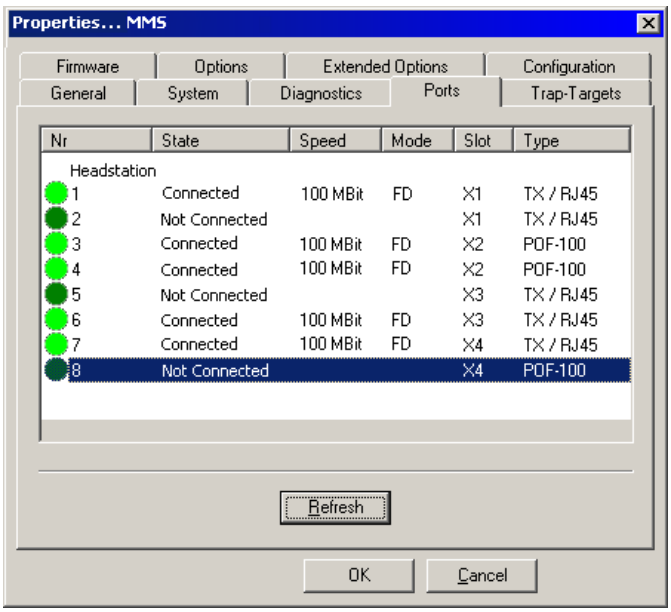


Figure 4-6 "Ports" menu

Comprehensive information, e.g., from interface types and states, through transmission data to port levels, is displayed here. All information is automatically created and updated.

Trap Targets

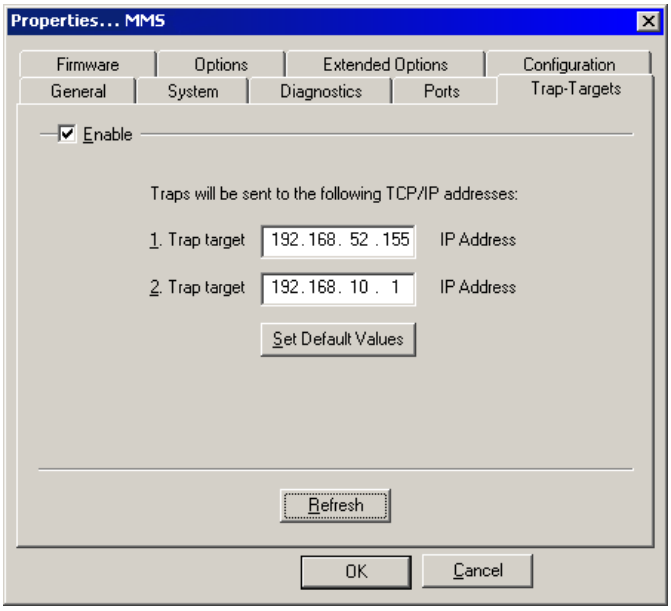


Figure 4-7 "Trap Targets" menu

Trap targets are displayed or set here, and the "send traps" function can be activated or deactivated. Clicking on "Set Default Values" automatically activates the IP address of the computer on which the Factory Manger is installed as the trap target.

Firmware

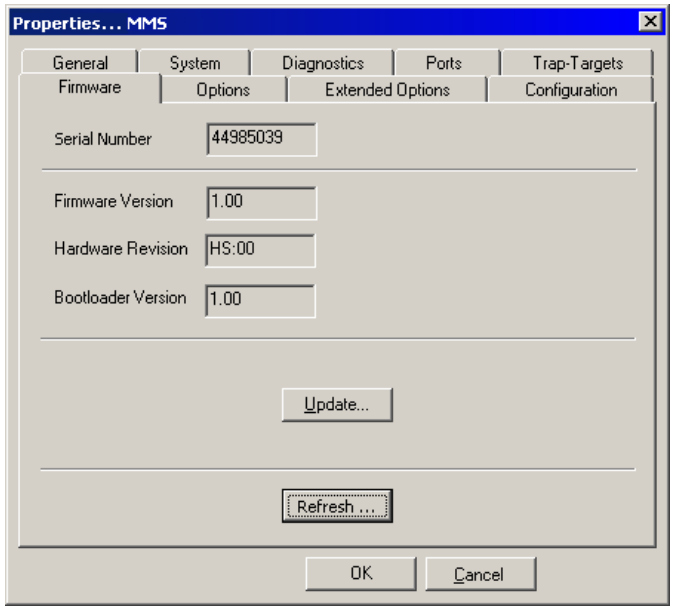


Figure 4-8 "Firmware" menu

Here you can view all information about the current device software (firmware). You can also update the software/firmware using the Factory Manager.

Firmware update

When you click on "Update", the following window appears, which contains information about the firmware used.

During a firmware update, the current status is shown on the MMS display:

03 - Downloading firmware via the network.

04 - Saving the firmware in the MMS Flash memory.

05 - The new firmware has been saved successfully.

Display goes out.

bo - Device is booting and loading new firmware in the RAM.

Following a firmware update, a reset is executed **automatically** to activate the new firmware.

Please make sure that the "TFTP Server" service program is activated in the toolbar.

You can monitor the download in the message window (25%, 50%, 75%, 100%). Always wait until all the LEDs light up after approximately two minutes and the device is available again after booting.

It is not ensured that all existing configuration data will be retained after a firmware update/downgrade. Therefore, please check the configuration settings or return the device to the settings default upon delivery.

A voltage failure during a firmware update results in the destruction of the firmware on the MMS. An update via XMODEM is required, see "Starting With Faulty Software (Firmware)" on page 4-120.

Update

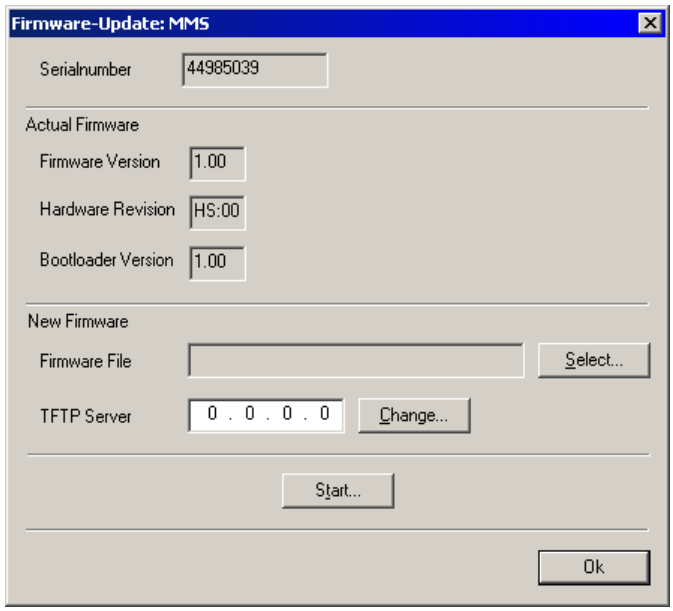


Figure 4-9 "Update" menu

In order to enable a firmware update, the firmware image must be located in the "Download" directory of the Factory Manager.

An application note for firmware update via TFTP (AH EN TFTP FIRMWARE UPDATE) can be found in the Download Center at www.download.phoenixcontact.com.

Options

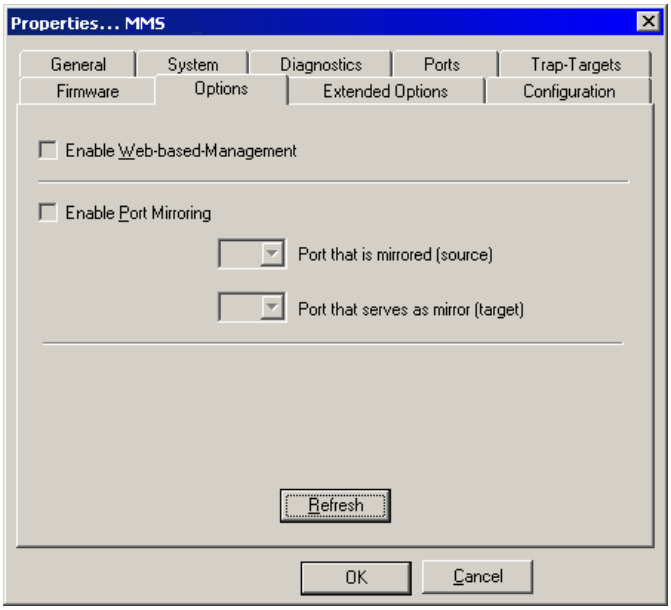


Figure 4-10 "Options" menu

Two functions are available for selection:

– Activate/deactivate the web server.
– Configure the port mirroring function.

If ports are set with the same value for the source and destination, port mirroring will be disabled. The source port is set to "0".

Enter the destination port in the relevant multicast group in order to enable multicast packets to be received at the set destination port.

Extended Options

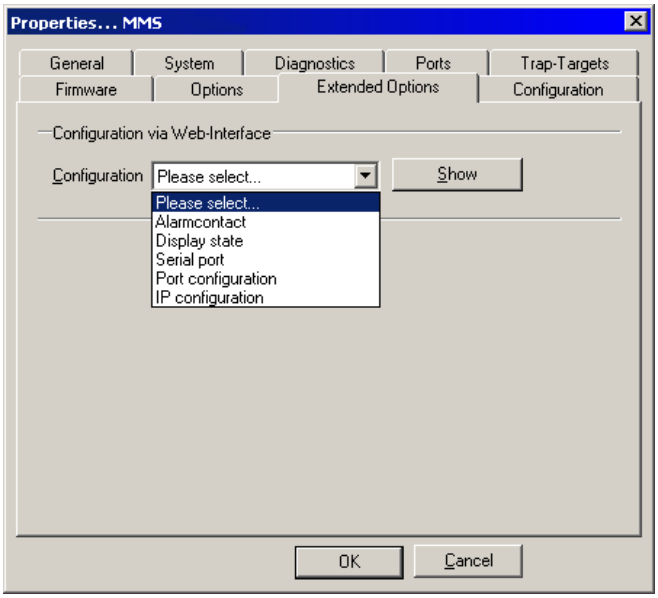


Figure 4-11 "Extended Options" menu

You can jump straight to the web interface from here via a selection menu. The relevant function is described in "Web-Based Management (WBM)" on page 4-11 and onwards.

Configuration

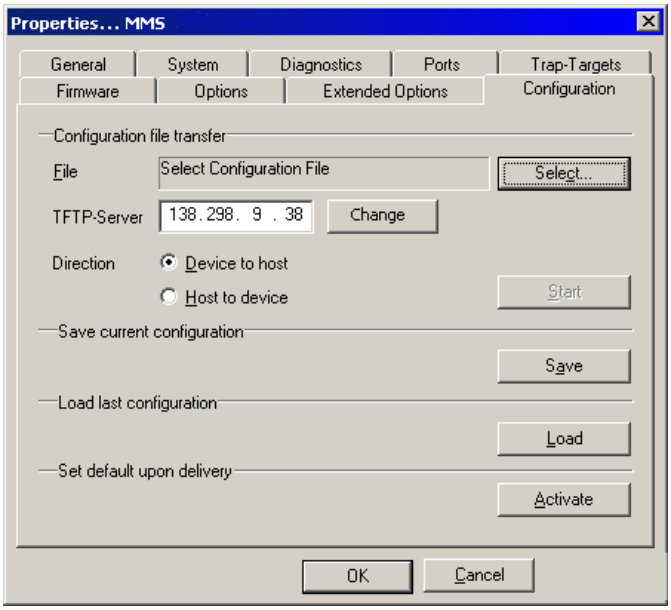


Figure 4-12 "Configuration" menu

Various options are provided here for saving or loading the configuration.

4.2 Web-Based Management (WBM)

4.2.1 General Function

Online diagnostics

The user-friendly web-based management interface can be used to manage the switch from anywhere in the network using a standard browser. Comprehensive configuration and diagnostic functions are clearly displayed on a graphic user interface. Every user with a network connection to the device has read access to that device via a browser. Depending on the physical structure of the switch, a wide range of information about the device itself, the set parameters, and the operating state can be viewed.

Modifications can only be made by entering the valid password. By default upon delivery, the password is "private".

For security reasons, we recommend you enter a new, unique password.

4.2.2 Requirements for the Use of WBM

As the web server operates using the Hyper Text Transfer Protocol, a standard browser can be used. Access is via the URL "http://IP address of the device".
Example: "http://172.16.29.112".
For full operation of the web pages, the browser must support JavaScript 1.2 and cascading style sheets Level 1. We recommend the use of Microsoft Internet Explorer 6.0.

WBM can only be called using a valid IP address. By default upon delivery, the switch has **no** valid IP address.

Settings are not automatically saved permanently. If the active configuration has not been saved, a flashing floppy disk icon appears in the top-right corner in WBM. The icon is linked to the "Configuration Management" web page. The active configuration can be saved permanently by selecting "Save current configuration" on this web page.

4.2.2.1 Structure of the Web Pages

The web pages are divided into four areas:

– Device type and device logo.
– Device name (assigned by the user) and loading time, to prevent mix-ups.
– Navigation tree on the left-hand side.
– Information tables, which contain current device information during runtime.

4.2.2.2 Password Concept

After having entered the valid password, no further entry of the password is necessary for a period of 300 s (default). After this period of time has elapsed or after clicking on "Logout", the password must be re-entered.

The period of time can be set using the "flWorkFWCtrlLoginExpire" SNMP object within a range of 30 s to 3600 s (default 300 s).

The concept is valid for the first ten users logged on at the same time. All other users must confirm each configuration modification by entering the password, until less than ten users are logged on.

4.2.3 Functions/Information in WBM

The navigation tree provides direct access to the following four areas:

– **General Instructions**
  Basic information about WBM.
– **Device Information**
  General device information.
– **General Configuration**
  Device configuration/device as a network device.
– **Switch Station**
  Device-specific configuration and diagnostics.

4.2.3.1 General Instructions

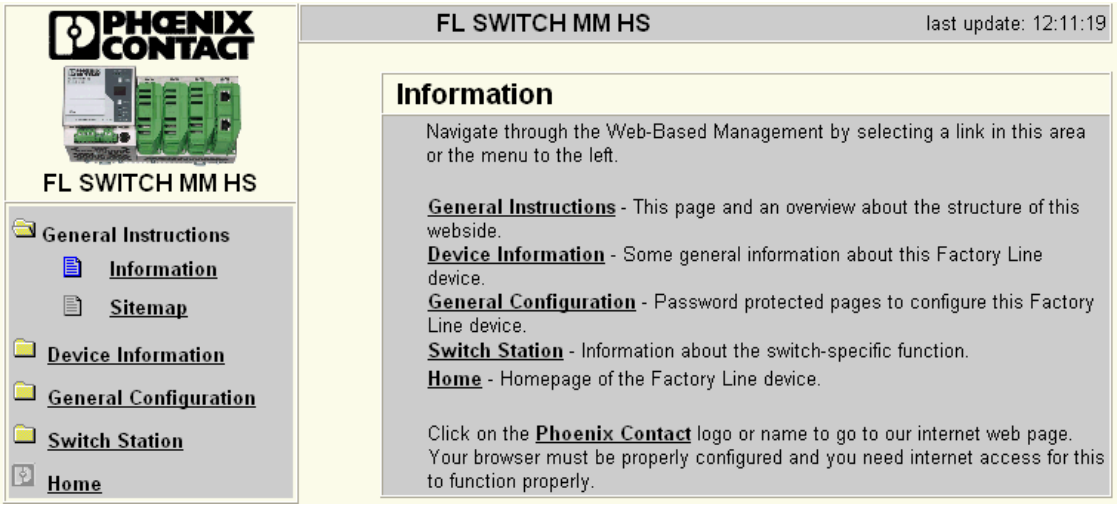

FL SWITCH MM HS
FL SWITCH MM HS
last update: 12:11:19
General Instructions
Information
Sitemap
Device Information
General Configuration
Switch Station
Home
Information
Navigate through the Web-Based Management by selecting a link in this area or the menu to the left.
General Instructions - This page and an overview about the structure of this webside.
Device Information - Some general information about this Factory Line device.
General Configuration - Password protected pages to configure this Factory Line device.
Switch Station - Information about the switch-specific function.
Home - Homepage of the Factory Line device.
Click on the Phoenix Contact logo or name to go to our internet web page. Your browser must be properly configured and you need internet access for this to function properly.

Figure 4-13 "Information" web page for the MMS

General Instructions

Contains a brief description of WBM and a navigation tree (site map), which is linked to every page of WBM.

4.2.3.2 Device Information

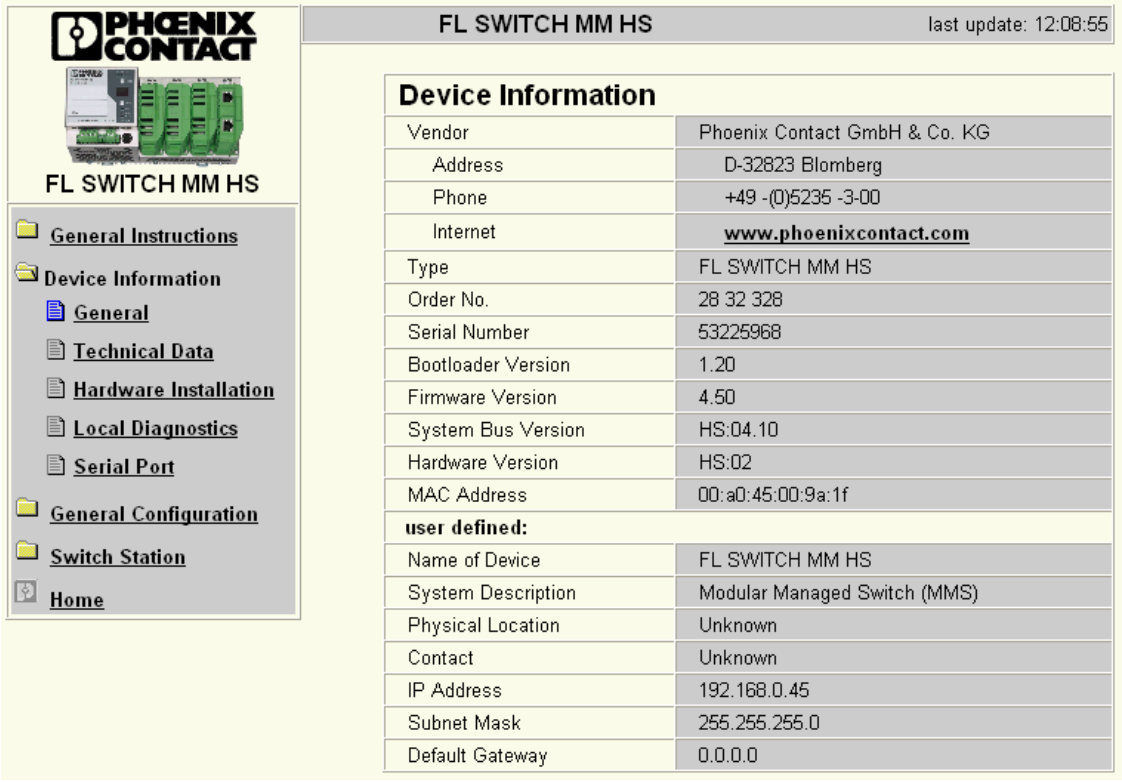


Figure 4-14 "Device Information" web page

"General" Menu
This page contains a range of static information about the device and the manufacturer.

"Technical Data" Menu
This page lists the main technical data.

"Hardware Installation" Menu
This page contains a connection diagram for connecting the redundant power supply and the alarm contact.

"Local Diagnostics" Menu
This page describes the meaning of the switchable diagnostic and status indicators, and lists the various display options for the 7-segment display.

"Serial Port" Menu
This page lists the transmission parameters for serial communication.

4.2.3.3 General Configuration

"IP Configuration" Menu

This page displays the set IP parameters, management VLAN ID, and addressing mechanism.

The management VLAN ID specifies in which VLAN the switch can be accessed if it is operating in "Tagging" VLAN mode.

To change the IP parameters via WBM, "Static" assignment must be selected.

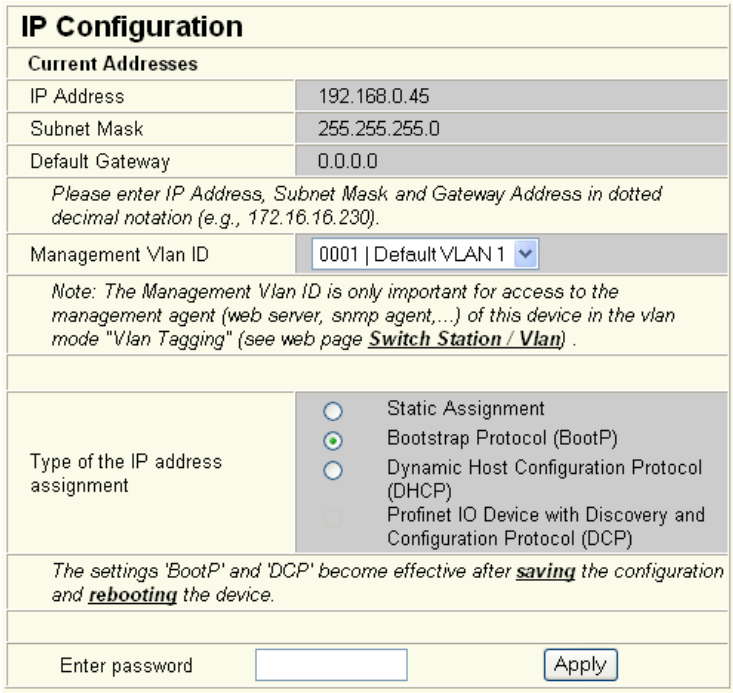

IP Configuration
Current Addresses
IP Address
192.168.0.45
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
Please enter IP Address, Subnet Mask and Gateway Address in dotted decimal notation (e.g., 172.16.16.230).
Management Vlan ID
0001 | Default VLAN 1
Note: The Management Vlan ID is only important for access to the management agent (web server, snmp agent,...) of this device in the vlan mode "Vlan Tagging" (see web page Switch Station / Vlan) .
Type of the IP address assignment
Static Assignment
Bootstrap Protocol (BootP)
Dynamic Host Configuration Protocol (DHCP)
Profinet IO Device with Discovery and Configuration Protocol (DCP)
The settings 'BootP' and 'DCP' become effective after saving the configuration and rebooting the device.
Enter password
Apply

Figure 4-15 "IP Configuration" web page

IP Address Assignment

While the switch waits for an IP address to be assigned - "01" or "dP" in the display - the mode LED selected via the mode button also flashes.

– Static Assignment
  The switch can be accessed using the set IP address and does not send any kind of requests on the receipt of IP parameters.

If you modify the IP address and/or the other IP parameters via WBM, once you click on "Apply" you will no longer have access via the IP address set in the browser.

– Bootstrap Protocol (BootP)
  The switch sends a BootP request after every restart and receives a BootP reply with IP parameters. If the BootP reply is disabled, the switch starts after the third request with the last IP parameters saved. If the switch has no saved IP parameters, the switch continues to send BootP requests until it receives a response with a BootP reply.

– Dynamic Host Configuration Protocol (DHCP)
  Once DHCP has been enabled, the switch attempts to apply network parameters from a DHCP server. The setting, regardless of whether DHCP is enabled or not, is saved permanently.

Once DHCP has been enabled, the display contains "01" and waits for IP parameters from a DHCP server. As long as no IP parameters have been assigned by a DHCP server, the switch can **still** be accessed via the previously set IP parameters.

– Discovery and Configuration Protocol (DCP)
  Mode for assigning IP addresses in PROFINET. After startup, the switch waits for the startup of the IO controller or an engineering tool. This status is indicated by display output "dP". The switch can only be accessed after configuration using the assigned IP address. The assigned IP address is not saved permanently, which means that the switch waits to be assigned an address every time the device starts. DCP is activated automatically if "Profinet" mode is selected.

If the MMS has established a PROFINET connection, a dot appears in the bottom-right corner of the display.

"System Identification" Menu
This menu is used to display or modify user-specific device data, e.g., location, device name or function. This device data is also available in SNMP.

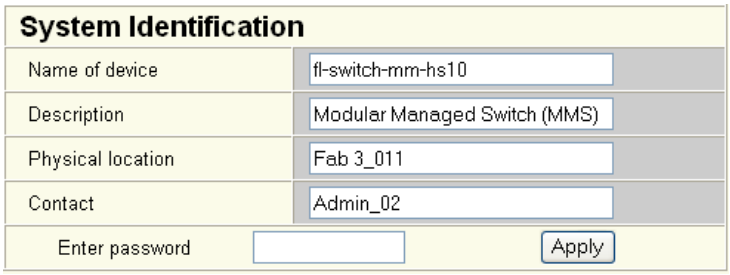
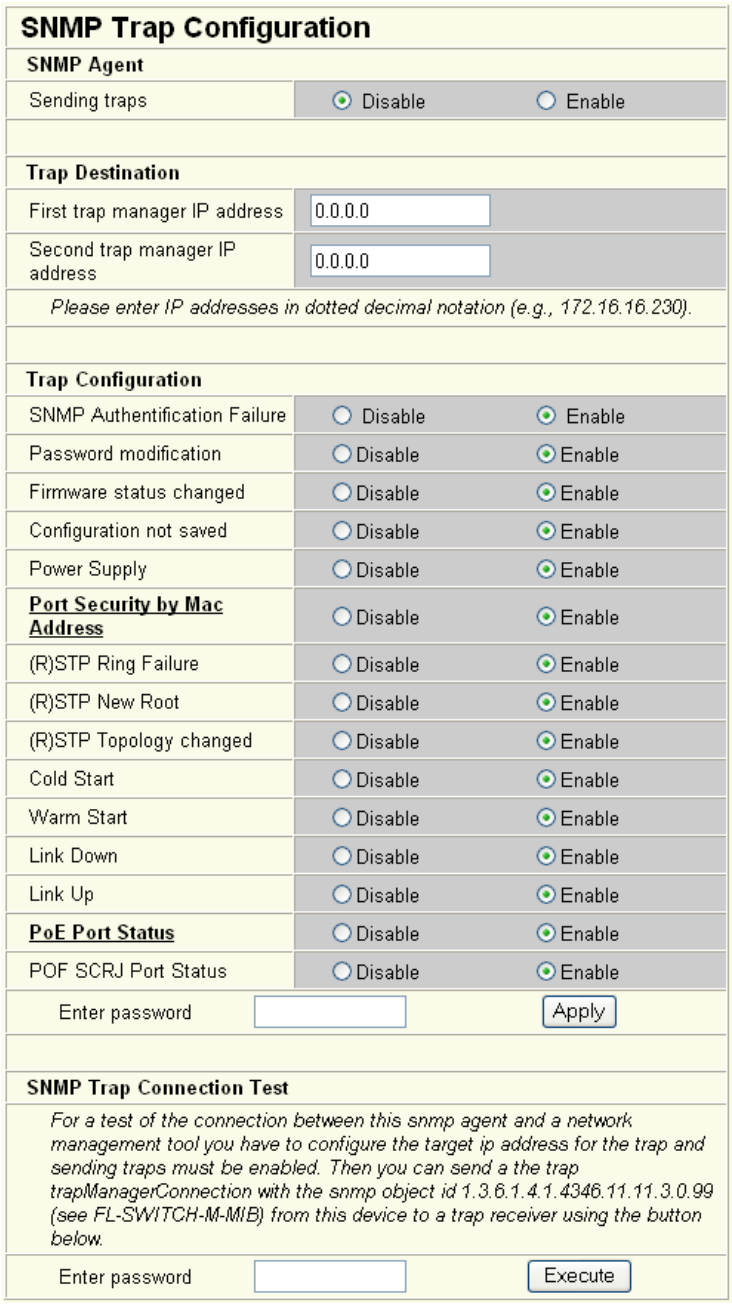


Figure 4-16 "System Identification" menu

"SNMP Trap Configuration" Menu

SNMP Agent The "send traps" function can be globally enabled/disabled here.



SNMP Trap Configuration

SNMP Agent		
Sending traps	◉ Disable	○ Enable
Trap Destination		
First trap manager IP address	0.0.0.0	
Second trap manager IP address	0.0.0.0	
Please enter IP addresses in dotted decimal notation (e.g., 172.16.16.230).		
Trap Configuration		
SNMP Authentification Failure	○ Disable	◉ Enable
Password modification	○ Disable	◉ Enable
Firmware status changed	○ Disable	◉ Enable
Configuration not saved	○ Disable	◉ Enable
Power Supply	○ Disable	◉ Enable
Port Security by Mac Address	○ Disable	◉ Enable
(R)STP Ring Failure	○ Disable	◉ Enable
(R)STP New Root	○ Disable	◉ Enable
(R)STP Topology changed	○ Disable	◉ Enable
Cold Start	○ Disable	◉ Enable
Warm Start	○ Disable	◉ Enable
Link Down	○ Disable	◉ Enable
Link Up	○ Disable	◉ Enable
PoE Port Status	○ Disable	◉ Enable
POF SCRJ Port Status	○ Disable	◉ Enable
Enter password		Apply
SNMP Trap Connection Test		
For a test of the connection between this snmp agent and a network management tool you have to configure the target ip address for the trap and sending traps must be enabled. Then you can send a the trap trapManagerConnection with the snmp object id 1.3.6.1.4.1.4346.11.11.3.0.99 (see FL-SWITCH-M-MIB) from this device to a trap receiver using the button below.		
Enter password		Execute

Figure 4-17 "SNMP Configuration" web page

Trap Destination This part of the table is used to view or modify the IP addresses of the two trap receivers.

Trap Configuration The "send traps" function can be disabled individually here.

SNMP Trap Connection Test Once the "send traps" function has been activated and the trap manager has been defined using the IP addresses, test traps can now be sent using "Execute" to test the communication path from the switch to the trap receiver.

"Software Update" Menu

This page is used to view or modify the parameters for a software update and to trigger the update.

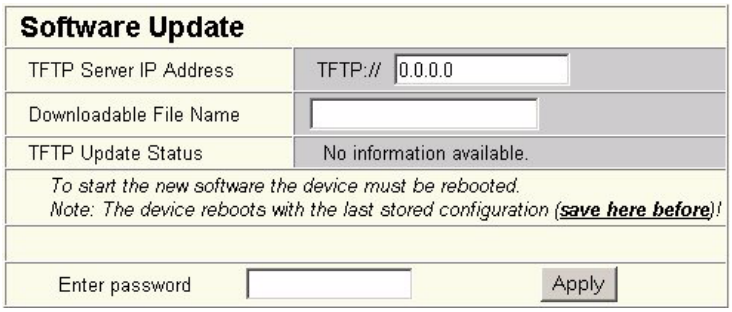

Software Update
TFTP Server IP Address
TFTP:// 0.0.0.0
Downloadable File Name
TFTP Update Status
No information available.
To start the new software the device must be rebooted.
Note: The device reboots with the last stored configuration (save here before)!
Enter password
Apply

Figure 4-18 "Software Update" web page

During a firmware update, the current status is shown on the MMS display:

03 - Downloading firmware via the network.

04 - Saving the firmware in the MMS Flash memory.

05 - The new firmware has been saved successfully.

Display goes out.

bo - Device is booting and loading new firmware in the RAM.

Following a firmware update, a reset is executed **automatically** to activate the new firmware.

Please make sure that the "TFTP Server" service program is activated in the Factory Manager toolbar.

You can monitor the download in the Factory Manager message window (25%, 50%, 75%, 100%). Always wait until all the LEDs light up after approximately two minutes and the device is available again after booting.

It is not ensured that all existing configuration data will be retained after a firmware update/downgrade. Therefore, please check the configuration settings or return the device to the settings default upon delivery.

A voltage failure during a firmware update results in the destruction of the firmware on the MMS. An update via XMODEM is required, see "Starting With Faulty Software (Firmware)" on page 4-120.

"Change Password" Menu

This option can be used to specify the current password and then enter a new, unique password. By default upon delivery, the password is "private" (please note that it is case-sensitive). For security reasons, the input fields do not display your password, but instead "*******" is displayed.

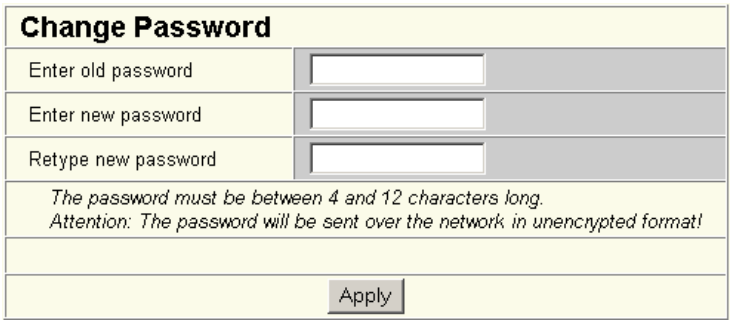

Change Password
Enter old password
Enter new password
Retype new password
The password must be between 4 and 12 characters long.
Attention: The password will be sent over the network in unencrypted format!
Apply

Figure 4-19 "Change Password" web page

The password must be between four and twelve characters long. Please note that the password is always transmitted via the network in unencrypted format.

Forgotten your password?
Call the Phoenix Contact phone number listed in the Appendix, making sure you have the device serial number and MAC address to hand.

"User Interfaces" Menu

The following actions can be executed here:

– Activation/deactivation of the Telnet server.
– Activation/deactivation of the web server.
– Activation/deactivation of the SNMP agent.
– Activation/deactivation of the configuration pages for redundancy mechanisms.
– Activation/deactivation of the configuration pages for multicast filtering.
– Activation/deactivation of the configuration pages for VLAN.
– Activation/deactivation of the configuration pages for the DHCP relay agent.

With the activation/deactivation of the configuration pages under "User Interfaces", only the web pages for configuring the selected functions are enabled/disabled in the WBM menu.

– Setting the refresh intervals for the automatic update of the web pages. Here, you can also set the refresh interval for automatic update of different web pages. If the interval is set to "0", the pages will no longer be updated.

Automatic update of web pages is only possible when using Internet Explorer Version 5.5 or later.

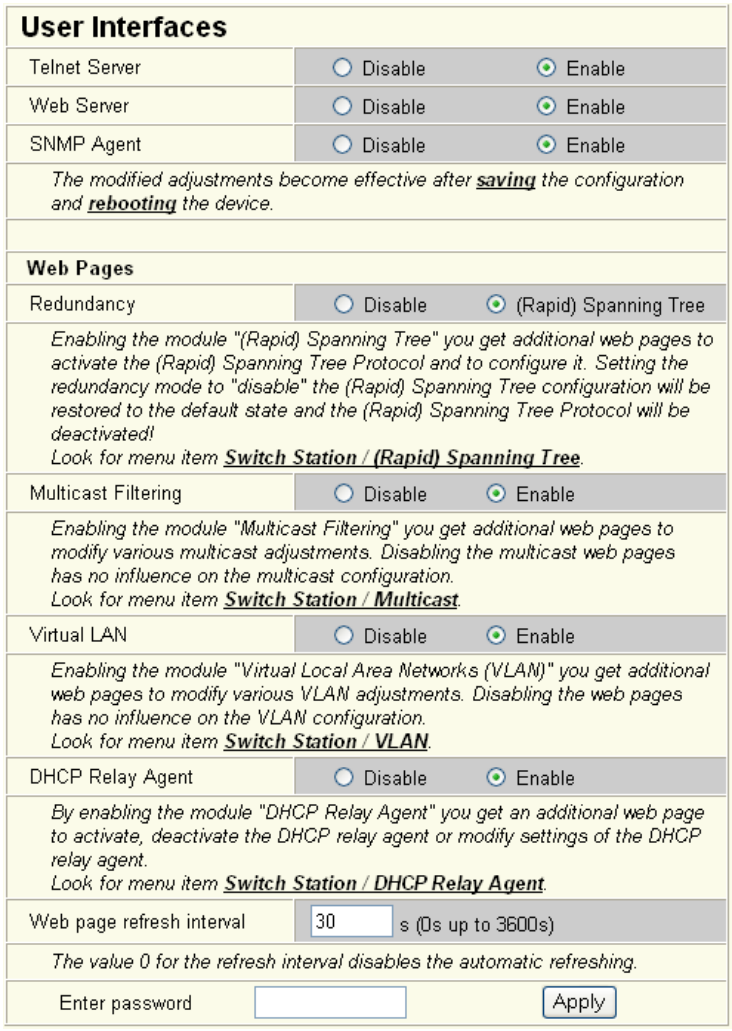

User Interfaces
Telnet Server
Disable
Enable
Web Server
Disable
Enable
SNMP Agent
Disable
Enable
The modified adjustments become effective after saving the configuration and rebooting the device.
Web Pages
Redundancy
Disable
(Rapid) Spanning Tree
Enabling the module "(Rapid) Spanning Tree" you get additional web pages to activate the (Rapid) Spanning Tree Protocol and to configure it. Setting the redundancy mode to "disable" the (Rapid) Spanning Tree configuration will be restored to the default state and the (Rapid) Spanning Tree Protocol will be deactivated!
Look for menu item Switch Station / (Rapid) Spanning Tree.
Multicast Filtering
Disable
Enable
Enabling the module "Multicast Filtering" you get additional web pages to modify various multicast adjustments. Disabling the multicast web pages has no influence on the multicast configuration.
Look for menu item Switch Station / Multicast.
Virtual LAN
Disable
Enable
Enabling the module "Virtual Local Area Networks (VLAN)" you get additional web pages to modify various VLAN adjustments. Disabling the web pages has no influence on the VLAN configuration.
Look for menu item Switch Station / VLAN.
DHCP Relay Agent
Disable
Enable
By enabling the module "DHCP Relay Agent" you get an additional web page to activate, deactivate the DHCP relay agent or modify settings of the DHCP relay agent.
Look for menu item Switch Station / DHCP Relay Agent.
Web page refresh interval
30
s (0s up to 3600s)
The value 0 for the refresh interval disables the automatic refreshing.
Enter password
Apply

Figure 4-20 "User Interfaces" web page

"Access Control" Menu

Here you can specify the IP addresses from which access to the web interface is permitted. To do so, enter the IP address in dotted notation and select whether read-only or read/write access is to be assigned. As an option, another name can be assigned under "Description". Access to WBM can be configured for a maximum of ten IP addresses.

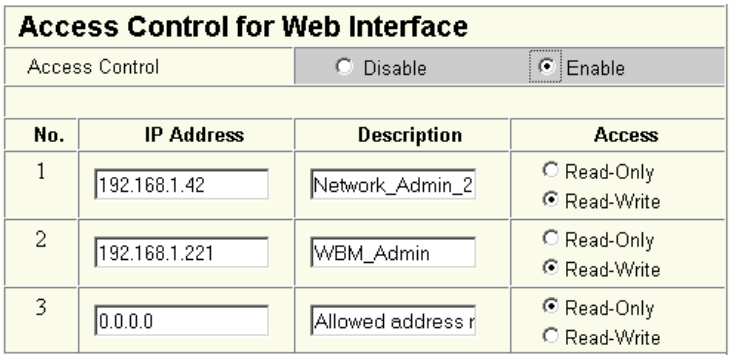


Figure 4-21 "Access Control for Web Interface" web page

Due to configuration errors, you may accidentally block your own access. In this case, you can disable access control via the **serial** interface using the "Access Control for Web" button.

"Operating Mode" Web Page

Operating as a PROFINET device

In this menu, select whether the switch is to operate as a PROFINET device. For additional information on operation as a PROFINET device, see Section 8 "Operating as a PROFINET Device".

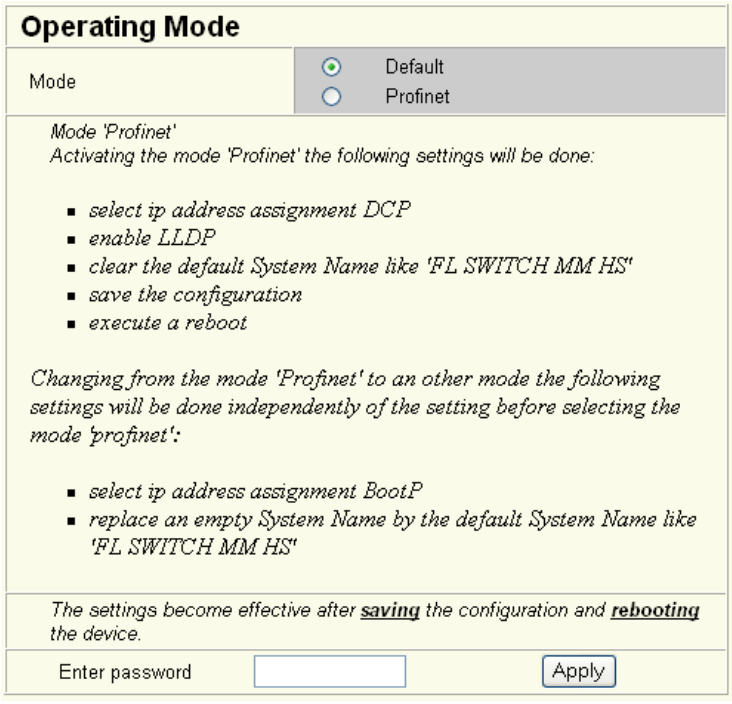

Operating Mode
Mode
Default
Profinet
Mode 'Profinet'
Activating the mode 'Profinet' the following settings will be done:
select ip address assignment DCP
enable LLDP
clear the default System Name like 'FL SWITCH MM HS"
save the configuration
execute a reboot
Changing from the mode 'Profinet' to an other mode the following settings will be done independently of the setting before selecting the mode 'profinet':
select ip address assignment BootP
replace an empty System Name by the default System Name like 'FL SWITCH MM HS"
The settings become effective after saving the configuration and rebooting the device.
Enter password
Apply

Figure 4-22 "Operating Mode" web page

"Configuration Management/General" Menu

This table is used to view all parameters that are required to save the active configuration or load a new configuration, and to modify them (by entering a valid password). It can also be used to restart the system with the relevant configuration.

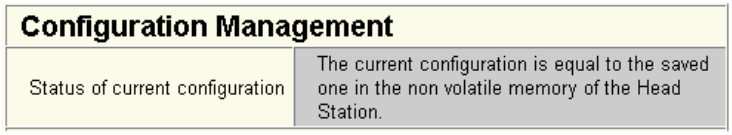

Configuration Management
Status of current configuration
The current configuration is equal to the saved one in the non volatile memory of the Head Station.

Figure 4-23 "Configuration Management" web page

Possible States for "Status of current configuration":

– The configuration has been modified but not saved (also indicated by the flashing floppy disk icon).
– Saving the current configuration.
– The current configuration is equal to the one saved in the non-volatile memory of the switch.
– The current configuration was saved.

Save current configuration

The active configuration together with the corresponding configuration name can be saved here by entering a valid password.

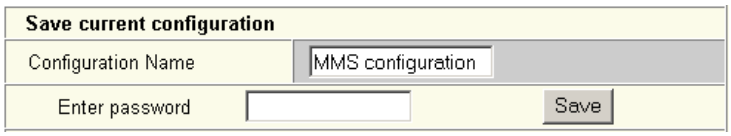


Figure 4-24 "Save current configuration" web page

If the new configuration is not activated by a reset after a configuration download, the "Save current configuration" command overwrites the previously loaded configuration and instead saves the active configuration of the MMS.

Set default upon delivery

This option can be used to reset the switch to its default settings (default upon delivery) by entering a valid password.

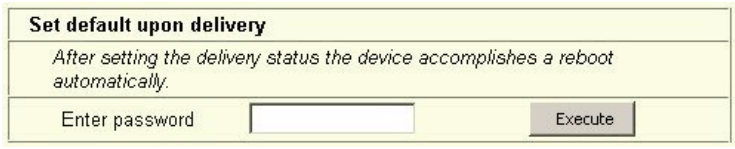

Set default upon delivery
After setting the delivery status the device accomplishes a reboot automatically.
Enter password
Execute

Figure 4-25 "Set default upon delivery" web page

WBM can only be called using a valid IP address. Once the switch has been reset to its default settings, it has **no** valid IP address and the addressing mechanism is set to BootP.

Load the last stored configuration

This option can be used to reactivate the last configuration saved in the memory module or on the device. All modifications made to the configuration since it was last saved are lost.

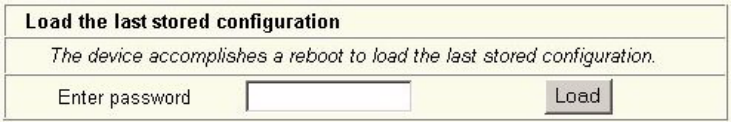

Load the last stored configuration
The device accomplishes a reboot to load the last stored configuration.
Enter password
Load

Figure 4-26 "Load the last stored configuration" web page

"Configuration Management/File Transfer" Menu

Configuration file transfer

This option can be used to save your device configuration on a PC or to operate the switch using a saved configuration.

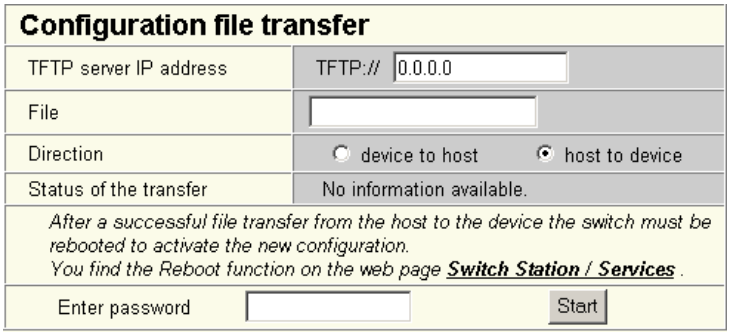

Configuration file transfer
TFTP server IP address
TFTP:// 0.0.0.0
File
Direction
device to host
host to device
Status of the transfer
No information available.
After a successful file transfer from the host to the device the switch must be rebooted to activate the new configuration.
You find the Reboot function on the web page Switch Station / Services .
Enter password
Start

Figure 4-27 "Configuration file transfer" web page

When a configuration is uploaded from the MMS to a PC, the last saved version is transmitted. If you want to transmit the active configuration, first save it again ("Save current configuration" function).

When a configuration is downloaded from the PC to a MMS, the new configuration is only activated once the switch has been reset.

The use of a configuration file does not affect an existing ("old") password.

Device Replacement

Configuration using a configuration file is used when replacing devices. To duplicate devices using a configuration file, observe the following:

– Create a point-to-point connection between a MMS and the management station.
– Load the configuration file on the MMS.
– Reset the MMS.
– Adjust the IP parameters.
– Save the configuration ("Save current configuration" function).

The duplicated switch can now be operated in the network using the adjusted IP parameters.

"Configuration Management/Memory Module" Menu

This web page provides an overview of the configuration in the memory module and indicates which configuration was used during booting.

Memory Module

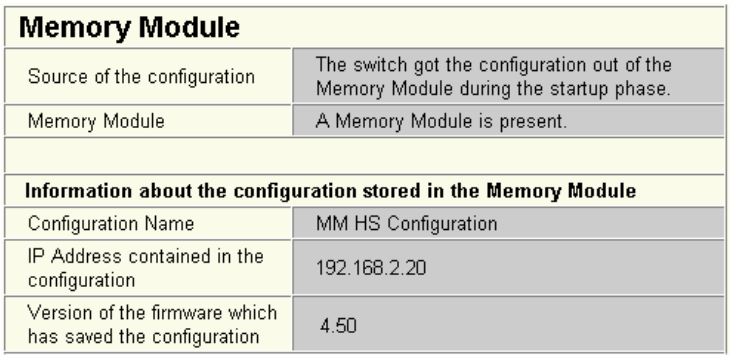

Memory Module
Source of the configuration
The switch got the configuration out of the Memory Module during the startup phase.
Memory Module
A Memory Module is present.
Information about the configuration stored in the Memory Module
Configuration Name
MM HS Configuration
IP Address contained in the configuration
192.168.2.20
Version of the firmware which has saved the configuration
4.50

Figure 4-28 "Memory Module" web page

Configuration comparison

Here you can compare the configuration on the memory module with the configuration in the head station memory. The result is displayed in text format. In addition, the result is displayed in encoded form (see also "Meaning of the 7-Segment Display" on page 1-14).

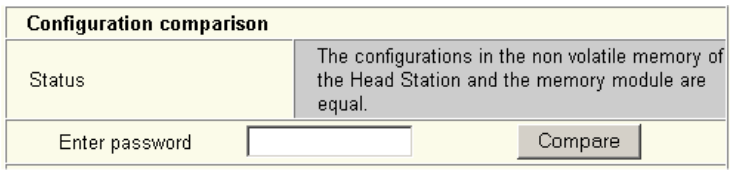

Configuration comparison
Status
The configurations in the non volatile memory of the Head Station and the memory module are equal.
Enter password
Compare

Figure 4-29 "Configuration comparison" web page

If you replace the memory module with another memory module within a few seconds, there is no need to update the configuration comparison manually.

Clear Memory Module

Here, you can delete the memory module by entering a valid password.

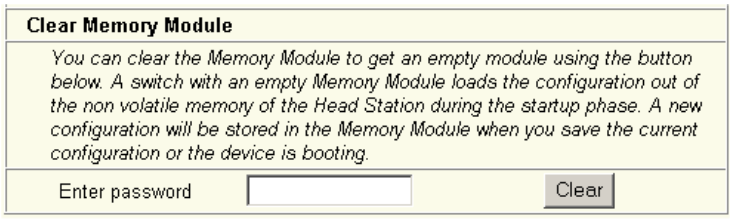

Clear Memory Module
You can clear the Memory Module to get an empty module using the button below. A switch with an empty Memory Module loads the configuration out of the non volatile memory of the Head Station during the startup phase. A new configuration will be stored in the Memory Module when you save the current configuration or the device is booting.
Enter password
Clear

Figure 4-30 "Clear Memory Module" web page

4.2.3.4 Switch Station

"Services" Menu

Reboot To trigger a reboot via the web interface, enter a valid password. Save the configuration beforehand, so that configuration modifications are retained or can be activated via a restart.

Port security status Here you can globally activate/deactivate the port security function. The settings for the individual ports can be made on the "Port/Port Security" web page.

Illegal Address Counter

Here you can reset the counter that records the unauthorized access attempts to the device.

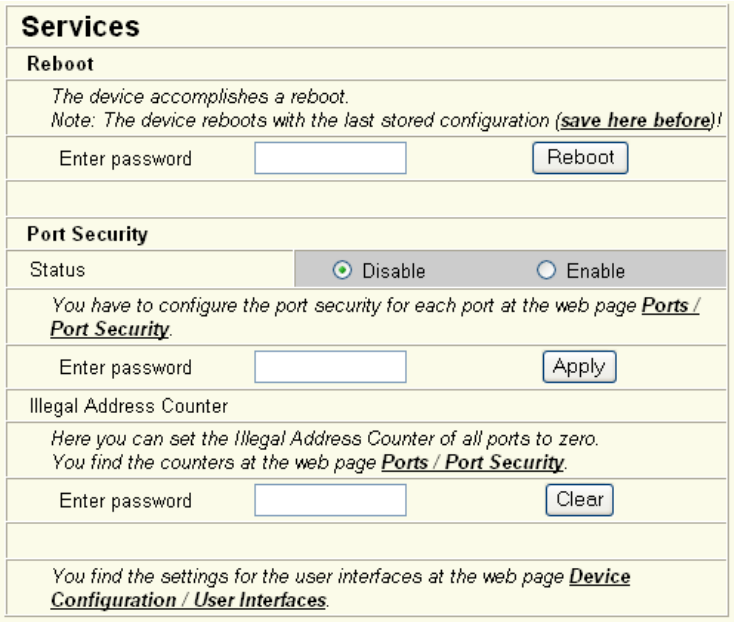

Services
Reboot
The device accomplishes a reboot.
Note: The device reboots with the last stored configuration (save here before)!
Enter password
Reboot
Port Security
Status
Disable
Enable
You have to configure the port security for each port at the web page Ports / Port Security.
Enter password
Apply
Illegal Address Counter
Here you can set the Illegal Address Counter of all ports to zero.
You find the counters at the web page Ports / Port Security.
Enter password
Clear
You find the settings for the user interfaces at the web page Device Configuration / User Interfaces.

Figure 4-31 "Services" web page

"DHCP Relay Agent" Menu

In this menu, the DHCP relay agent can be activated/deactivated according to the port, the corresponding address of the DHCP server can be entered, and the type of remote ID can be configured.

For additional information on the function of the DHCP relay agent, please refer to "DHCP Relay Agent" on page 10-1.

"Ports/Port Table" Menu

Overview of all available ports. Clicking on the relevant port number opens a port-specific page ("Port Configuration").

Port Table

Module	Interface	Port	Type	Port Status	Link State
HS	X1	1	TX 10/100	enable	100 MBit FD
		2	TX 10/100	enable	100 MBit FD
	X2	3	TX 10/100 MEM	enable	not connected
		4	TX 10/100 MEM	enable	not connected
	X3	5	empty	enable	not connected
		6	empty	enable	not connected
	X4	7	empty	enable	not connected
		8	empty	enable	not connected

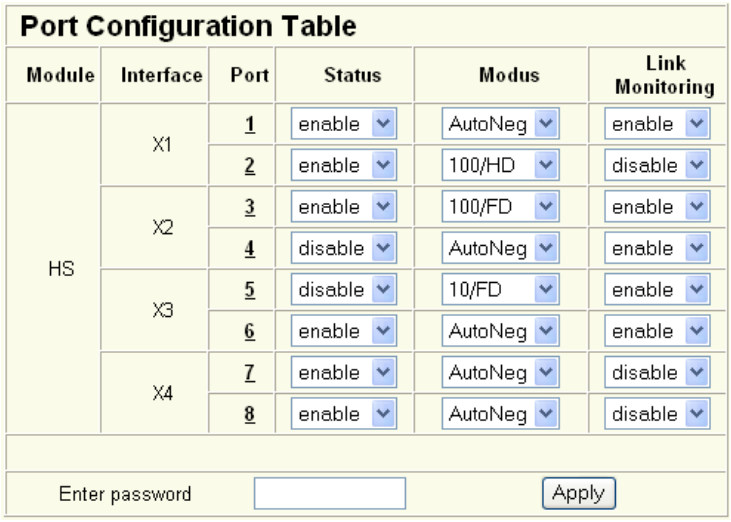
Note: This web page will be refreshed in 20 sec automatically (change the interval at the web page 'Services')!

Figure 4-32 "Port Table" web page

When setting the transmission mode, make sure that the same settings have been made at both ends of the connection. If the settings are not the same, this can result in increased collisions or CRC errors and can adversely affect network performance.

"Ports/Port Configuration Table" Menu

This menu provides an overview of the important configuration settings for all ports and also provides the option to set the status, transmission mode, and link monitoring function for all existing ports.



Port Configuration Table

Module	Interface	Port	Status	Modus	Link Monitoring
HS	X1	1	enable	AutoNeg	enable
		2	enable	100/HD	disable
	X2	3	enable	100/FD	enable
		4	disable	AutoNeg	enable
	X3	5	disable	10/FD	enable
		6	enable	AutoNeg	enable
	X4	7	enable	AutoNeg	disable
		8	enable	AutoNeg	disable

Enter password Apply

Figure 4-33 "Port Configuration Table" web page

"Ports/Port Configuration" Menu

Offers individual configuration options for each port.

Even if the port is switched off, the Link LED for the port remains active.

.

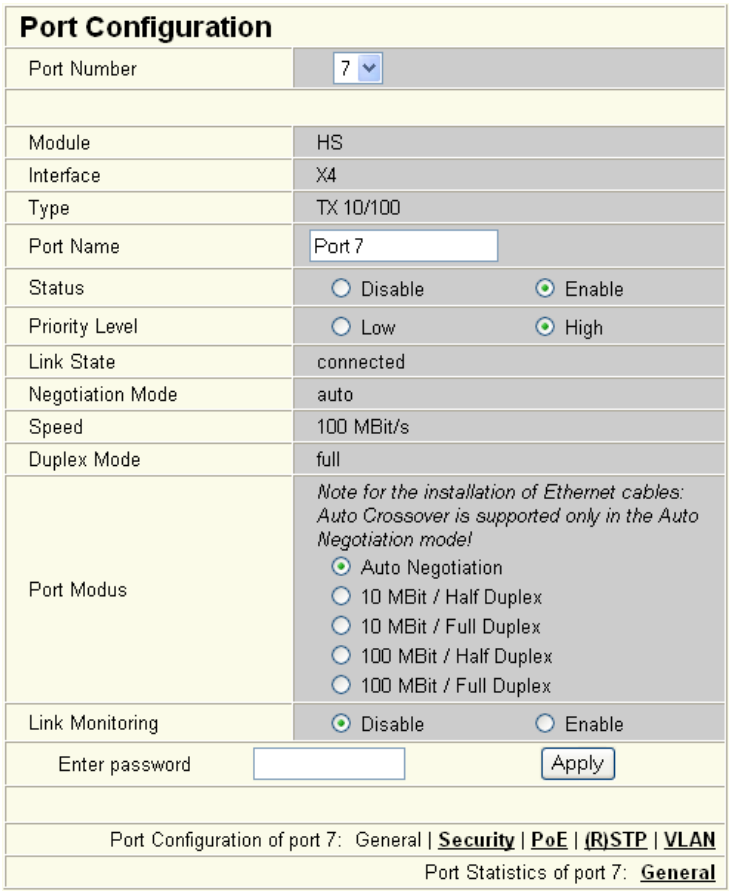
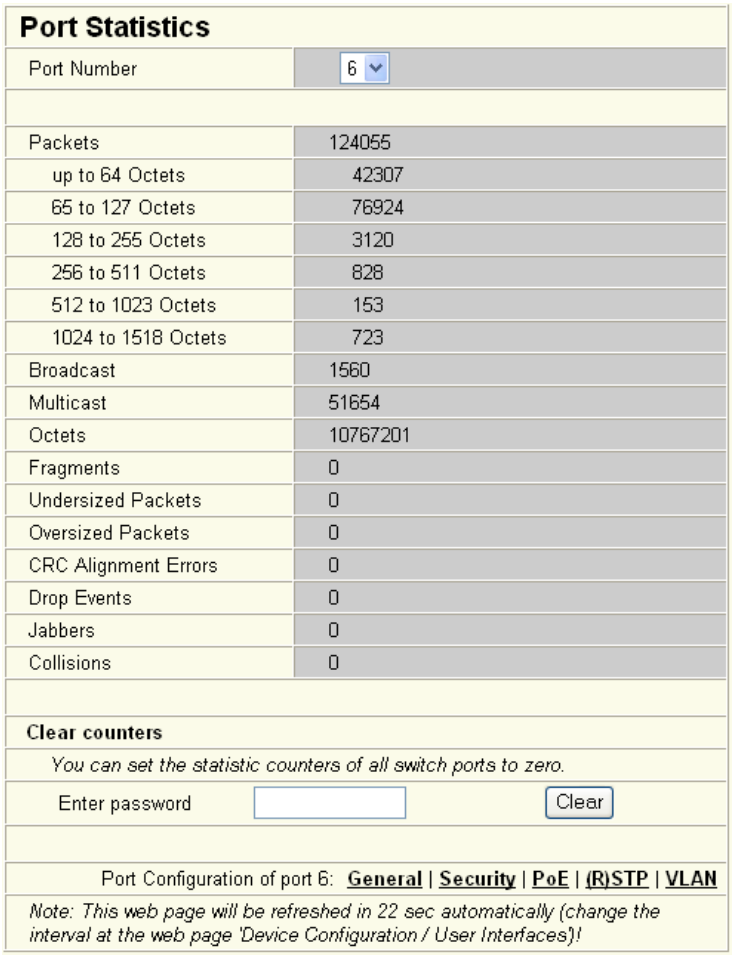


Figure 4-34 "Port Configuration" web page

"Ports/Port Statistics" Menu

This menu provides detailed statistical information about the volume of data for each individual port. On this page, additional counter states can be set to zero for all ports.

.



Port Statistics

Port Number	6
Packets	124055
up to 64 Octets	42307
65 to 127 Octets	76924
128 to 255 Octets	3120
256 to 511 Octets	828
512 to 1023 Octets	153
1024 to 1518 Octets	723
Broadcast	1560
Multicast	51654
Octets	10767201
Fragments	0
Undersized Packets	0
Oversized Packets	0
CRC Alignment Errors	0
Drop Events	0
Jabbers	0
Collisions	0

Clear counters

You can set the statistic counters of all switch ports to zero.

Enter password [ ] Clear

Port Configuration of port 6: General | Security | PoE | (R)STP | VLAN

Note: This web page will be refreshed in 22 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces)!

Figure 4-35 "Port Statistics" web page

"Ports/POF Port Table" Menu

The information available for the POF-SCRJ interface modules is displayed on this page.

POF-SCRJ transceiver diagnostics Port Table

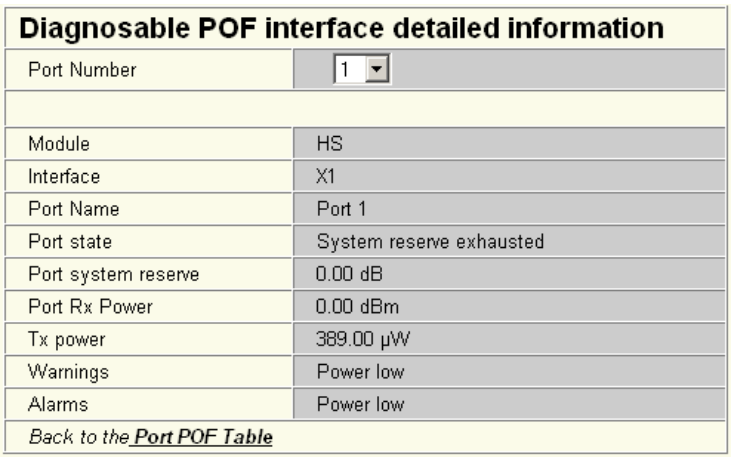
Module	Interface	Port	Transceiver status	RX system reserve
HS	X1	1 (details)	System reserve exhausted	System Reserve is 0.00 dB
		2 (details)	System reserve exhausted	System Reserve is 0.00 dB
	X2	3 (details)	System reserve exhausted	System Reserve is 0.00 dB
		4 (details)	System reserve exhausted	System Reserve is 0.00 dB
	X3	5 (details)	No diagnosable POF module plugged on this port	
		6 (details)	No diagnosable POF module plugged on this port	

Figure 4-36 "POF-SCRJ transceiver diagnostics Port Table" web page

The following states can be displayed under "Transceiver status":

– "System Hardware does not support diagnosable POF modules" (this hardware does not support POF-SCRJ diagnostics)
– "No POF-SCRJ Interface modules present" (no POF-SCRJ module is plugged in)
– "POF-SCRJ Interface module is present and OK" (the system reserve is greater than 2 dB and is displayed under "RX system reserve")
– "POF-SCRJ Interface module is present, but the system reserve is low" (the system reserve is less than 2 dB, but greater than 0 dB)
– "POF-SCRJ Interface module is present, but the system reserve is exhausted" (no system reserve available - the received optical power is below the required minimum value)

When you click on "details" under the port number, detailed information about the transmit/receive properties of the relevant port are displayed in the following window.



Diagnosable POF interface detailed information

Port Number	1
Module	HS
Interface	X1
Port Name	Port 1
Port state	System reserve exhausted
Port system reserve	0.00 dB
Port Rx Power	0.00 dBm
Tx power	389.00 µW
Warnings	Power low
Alarms	Power low
Back to the ***Port POF Table***	

Figure 4-37 "Diagnostics" web page

"Ports/Port Mirroring" Menu

Activation/deactivation and setting of port mirroring. Port mirroring is used to passively read data that is being transmitted via a selected port. To do this a measuring instrument (PC) is connected to the destination port, which records the data, yet must not itself be activated.

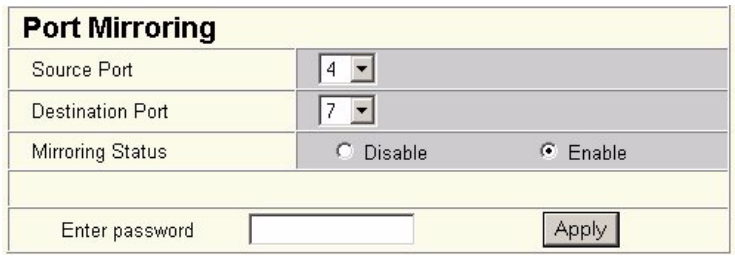


Figure 4-38 "Port Mirroring" web page

If ports are set with the same value, port mirroring will be disabled. The source port is set to "0".

Multicast data packets of created multicast groups cannot be mirrored. Enter the destination port in the relevant multicast group in order to enable multicast packets to be received at the set destination port.

The port capacity is calculated according to the set transmission parameters. Example: A source port is operated at 100 Mbps and reaches a capacity of 5%. The destination port is operated at 10 Mbps. Therefore, with the same volume of data the destination port reaches a capacity of 50%.

"Ports/Port Security" Menu

In order to make individual settings for each port, the "Port Security" function on the "Switch Station/Services" page must first be activated. The following options can be selected under "Security Mode":

– None
  No security settings for this port.
– Trap only
  When a disabled MAC address accesses a port, a trap is sent to the pre-defined trap targets. The port is not blocked.

A trap is sent for each MAC address that accesses a port illegally. If this MAC address accesses this port again after the aging time has elapsed and the MAC address has been deleted from the MAC address table, another trap is sent. However, if the duration of illegal access is shorter than the aging time, only one trap is sent following the first access attempt.

– Block packets
  Having received unauthorized packets, the port is blocked for all packets. A trap is sent, which indicates the unauthorized access attempt. The port remains blocked until the block is lifted by the administrator using the "Unlock" button on the "Switch Station/Ports/Port Security" page

– Block packets with automatic reenabling
  Having received unauthorized packets, the port is blocked for all packets. A trap is sent, which indicates the unauthorized access attempt. After the aging time has elapsed, the port is reenabled automatically.

The "Port Security" function is only suitable for ports to which termination devices are connected. It is not recommended to use this function for backbone or uplink ports, especially if RSTP is activated.

Enter the enabled MAC addresses as well as a name under "Allowed MAC Addresses".

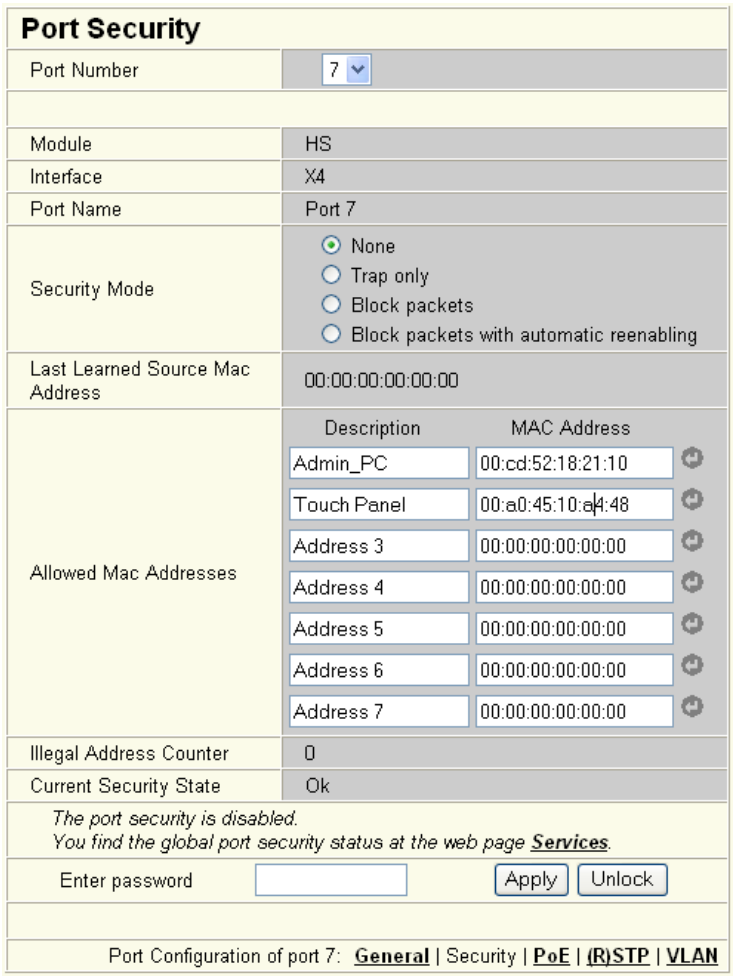


Figure 4-39 "Port Security" web page

The "Unlock" button can be used to disable the port block.

"Last Source MAC Address" indicates the last MAC address that accessed the port. If the port is blocked, the MAC address responsible for the block is indicated here.

"Ports/Power over Ethernet Port Table" Menu

This menu displays the available PoE status information for each port.

Power over Ethernet Port Table

Module	Interface	Port	PoE fault status	PoE operational status
HS	X1	1	No PoE enabled powered device connected to this port	
		2	No fault detected	Class 3 device
	X2	3	No PoE enabled powered device connected to this port	
		4	No PoE enabled powered device connected to this port	
	X3	5	Missing 48V supply fault	
		6	Missing 48V supply fault	

Figure 4-40 "Power over Ethernet Port Table" web page

The following states are supported:

– No error
– Error in the external PoE supply voltage
– Temperature too high
– Current limitation activated
– Load disconnected
– The PoE controller does not respond, 48 V supply may be missing
– No PoE interface module inserted in this slot
– The switch does not support PoE interface modules
– No PoE devices connected to this port
– Port Power over Ethernet Configuration

"Ports/Port Power over Ethernet Configuration" Menu

This menu can be used to set the port-specific configuration settings for Power over Ethernet.

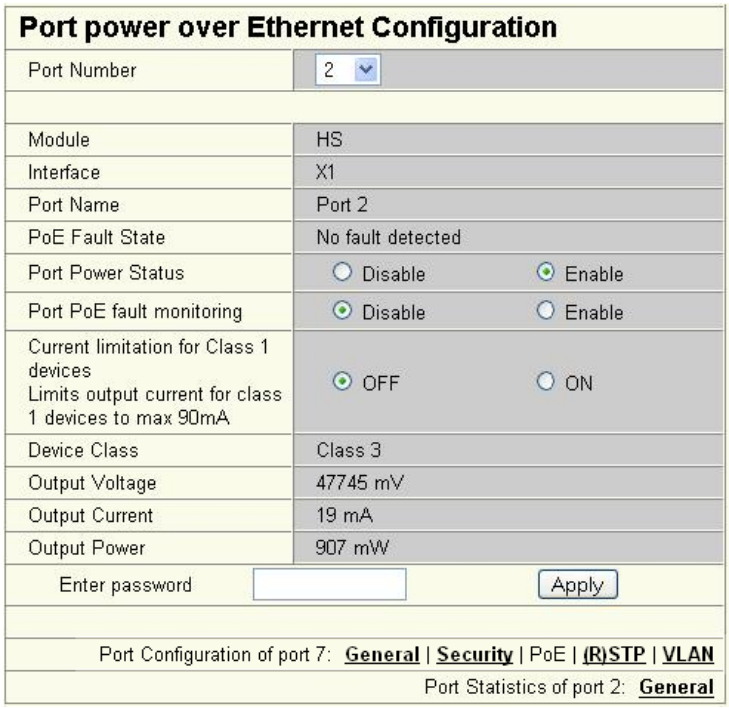
The PoE interface module is supported by firmware Version 4.0 or later. Firmware Versions < 4.0 treat the module as a standard RJ45 interface module. The module can operate in PoE mode without management and without support from the firmware and hardware (system bus). No configuration options or diagnostic data are available.

The use of the PoE interface module requires the application of system bus firmware 5.00 or later in the head station and system bus firmware 4.00 or later in the extension modules. If this requirement is not met in the head station or in any extension module, then PoE management is not available in the **entire** system. PoE interface modules can operate without management and without management support. No configuration options and no diagnostic data are available, connected termination devices are nevertheless supplied with power. The system bus firmware is displayed on the "Device Information/General" web page.

The PoE configuration options are also available if no PoE interface module is inserted. If a PoE interface module is inserted, the configuration is transmitted to the module after a few seconds.

Features of PoE Mode

– Up to twelve PoE interface modules with a total of 24 ports can be operated at the same time in an MMS.
– Configuration transmission on the interface module is only possible if there is a connected 48 V supply.
– The following management functions are available:
  - Display error states for each port and communicate via the alarm contact (yes/no)
  - Connect/disconnect voltage for each port
  - Current limitation for loads classified as Class 1 devices
– The following diagnostic information is displayed:
  - No error
  - Surge voltage/undervoltage
  - Thermal error
  - Overload
  - Disconnected load (the current consumption at this port is less than 10 mA, the supply voltage is disconnected by the PoE module)
  - No 48 V supply
  - No PoE termination device connected
  - No PoE interface module detected at this port
  - No hardware support due to the system bus
  - Detected class of a connected termination device (Class 0 to Class 4)
  - Output voltage and output current



Port power over Ethernet Configuration

Port Number	2
Module	HS
Interface	X1
Port Name	Port 2
PoE Fault State	No fault detected
Port Power Status	○ Disable ◉ Enable
Port PoE fault monitoring	◉ Disable ○ Enable
Current limitation for Class 1 devices Limits output current for class 1 devices to max 90mA	◉ OFF ○ ON
Device Class	Class 3
Output Voltage	47745 mV
Output Current	19 mA
Output Power	907 mW
Enter password	Apply

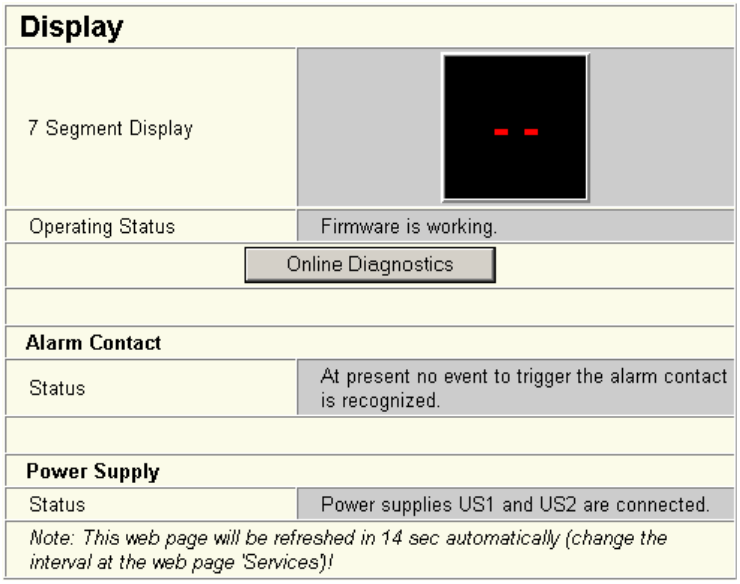
Port Configuration of port 7: **General** | **Security** | PoE | **(R)STP** | **VLAN**

Port Statistics of port 2: **General**

Figure 4-41 "Port Power over Ethernet Configuration" web page

"Diagnostics/Display" Menu

Current display of the 7-segment display, and the states of the alarm contact and redundant power supply.



Display

7 Segment Display	- -
Operating Status	Firmware is working.
Online Diagnostics	
Alarm Contact	
Status	At present no event to trigger the alarm contact is recognized.
Power Supply	
Status	Power supplies US1 and US2 are connected.

Note: This web page will be refreshed in 14 sec automatically (change the interval at the web page 'Services')!

Figure 4-42 "Display" web page

Click on "Online Diagnostics" to display the current view of the diagnostic display in a small browser window. The display is renewed automatically after two seconds.

"Diagnostics/Alarm Contact" Menu

Here, you can set whether and for which events the alarm contact can be used.

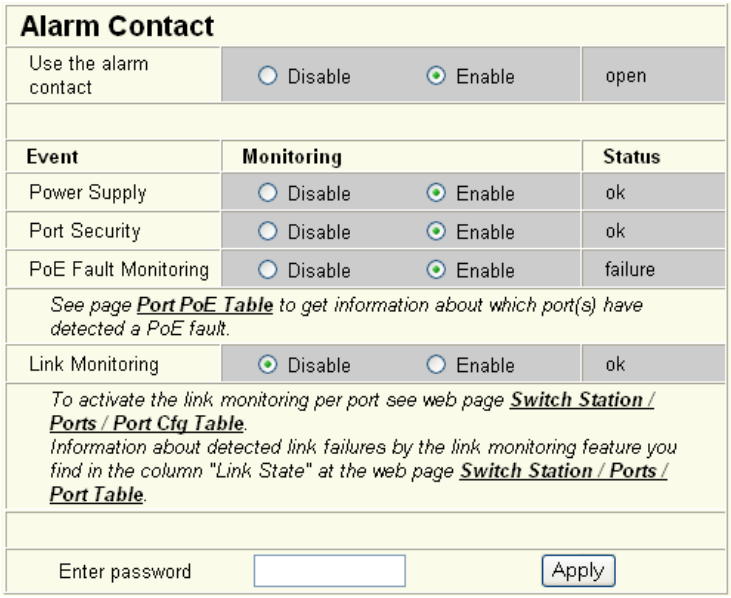


Figure 4-43 "Alarm Contact" web page

Click on the "Switch Station / Ports / Port Cfg Table" link (on "Alarm Contact" page in WBM) to access the port configuration page.

"Diagnostics/Utilization" Menu

Here, the network capacity of each individual port is displayed as a bargraph. The display is automatically updated according to the refresh interval.

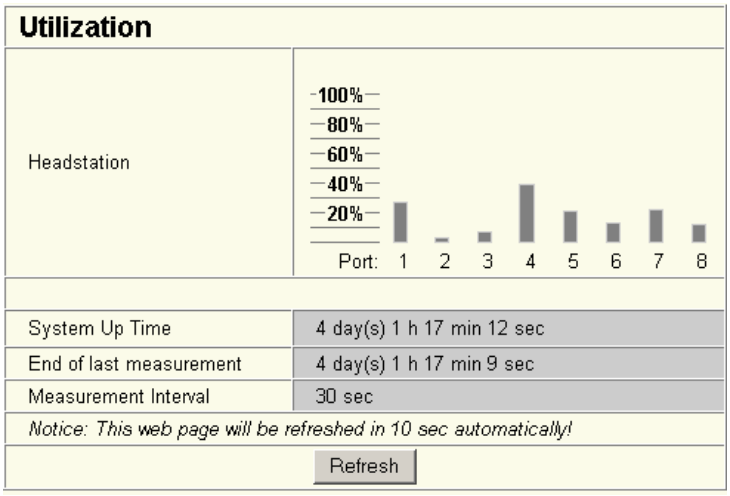


Figure 4-44 "Utilization" web page

Please note that the % scale is spread according to the capacity utilization.

"Diagnostics/Event Table" Menu

Here, you will find a list of the latest important events. The list contains up to 200 entries, from the 200th entry and onwards the oldest entries are overwritten (FIFO principle - first in, first out). If old entries are overwritten by new entries, a corresponding note is displayed under the event table.

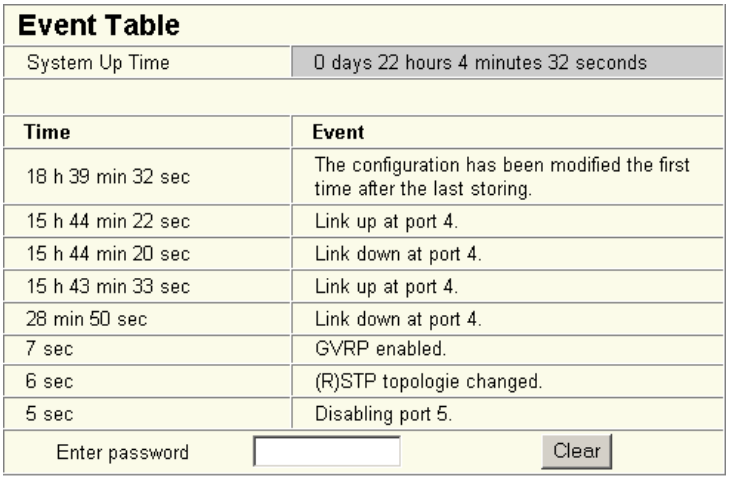

Event Table
System Up Time
0 days 22 hours 4 minutes 32 seconds
Time
Event
18 h 39 min 32 sec
The configuration has been modified the first time after the last storing.
15 h 44 min 22 sec
Link up at port 4.
15 h 44 min 20 sec
Link down at port 4.
15 h 43 min 33 sec
Link up at port 4.
28 min 50 sec
Link down at port 4.
7 sec
GVRP enabled.
6 sec
(R)STP topologie changed.
5 sec
Disabling port 5.
Enter password
Clear

Figure 4-45 "Event Table" web page

The "Clear" button can be used to delete entries in the event table.

The following events are listed in the event table:

- Event Table cleared.
- Password has been changed.
- Password has not been changed successfully.
- Configuration has been saved.
- The configuration has been modified the first time after the last storing.
- Memory Module recognized.
- Memory Module removed.
- Memory Module cleared.
- Configuration File Transfer successfully executed.
- Configuration File Transfer was not successfully executed.
- Firmware Update was successfully executed.
- Firmware Update was not successfully executed.
- Link up at port xy.
- Link down at port xy.
- Enabling port xy.
- Disabling port xy.
- Unpermitted mac address at port xy.
- RSTP enabled.
- RSTP disabled.
- RSTP topology changed.
- RSTP elected this switch as new root.
- IGMP Snooping enabled.
- IGMP Snooping disabled.
- IGMP Querier enabled.
- IGMP Querier disabled.
- Better query received.
- Better query received in vlan xy.
- Become active querier.
- Become active querier in vlan xy.
- GVRP enabled.
- GVRP disabled.
- Power Supply US1 lost.
- Power Supply US2 lost.
- Power Supply US1 and US2 are connected now.
- LLDP Agent enabled.
- LLDP Agent disabled.
- LLDP recognized new neighbor at port xy.
- LLDP neighborhood information changed at port xy.
- LLDP neighbor information become obsolete at port xy.
- Power over Ethernet fault detected at least one port.
- No Power over Ethernet faults detected any more.
- One of the interface modules is not supported by the system hardware. The interface will be able to send or receive data but cannot be diagnosed.
- A Profinet connection was established.

– The Profinet connection was terminated.
– Diagnosable POF module: OK on port xy.
– Diagnosable POF module: Warning level reached on port xy.
– Diagnosable POF module: Critical status on port xy.
– Configuration difference detected.
– Configuration difference detected at slot.
– Configuration difference removed.

"Diagnostics/MAC Address Table" Menu

Here, you will find a list of which MAC address has been detected at which switch port and its VLAN ID. If no packets are received at a port for a duration longer than the aging time, the entry is deleted.

Export as an Excel worksheet is possible via download. Thus an efficient analysis option is available that is especially helpful in larger networks.

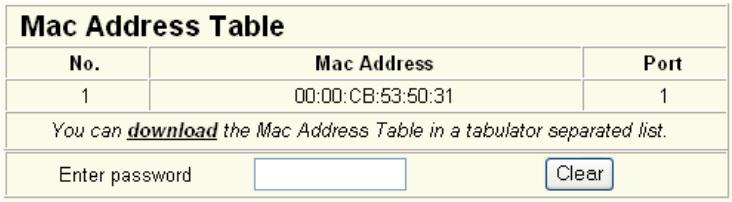


Figure 4-46 "MAC Address Table" web page

The "Clear" button can be used to delete entries in the MAC address table.

"Diagnostics/LLDP" Menu

For information about LLDP, please refer to "LLDP (Link Layer Discovery Protocol)" on page 9-1.

4.2.3.5 (Rapid) Spanning Tree/Multicast Filtering/VLAN

For information about (Rapid) Spanning Tree, please refer to Section 5 "(Rapid) Spanning Tree".

For information about multicast filtering, please refer to Section 6 "Multicast Filtering".

For information about the VLAN function, please refer to Section 7 "Virtual Local Area Network (VLAN)".

4.3 Simple Network Management Protocol (SNMP)

4.3.1 General Function

SNMP is a manufacturer-independent standard for Ethernet management. It defines commands for reading and writing information and defines formats for error and status messages. SNMP is also a structured model, which comprises agents and their relevant MIB (Management Information Base) and a manager. The manager is a software tool, which is executed on a network management station. The agents are located inside switches, bus terminals, routers, and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager regularly requests and displays this information. The devices can be configured by writing data from the manager to the MIB. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

All configuration modifications, which are to take effect after an MMS restart, must be saved permanently using the "flWorkFWCtrlConfSave" object.

SNMP Interface

All managed Factory Line components have an SNMP agent. This agent of an FL SWITCH MM HS manages Management Information Base II (MIB 2) according to RFC1213, RMON MIB, bridge MIB, If MIB, Etherlike MIB, Iana-address-family MIB, IANAifType MIB, SNMPv2 MIB, SNMP-FRAMEWORK MIB, P bridge MIB, Q bridge MIB, RSTP MIB, LLDP MIB, and private SNMP objects from Phoenix Contact (FL-SWITCH-M MIB).

Network management stations, such as a PC with the Factory Manager, can read and modify configuration and diagnostic data from network devices via the Simple Network Management Protocol (SNMP). In addition, any SNMP tools or network management tools can be used to access Factory Line products via SNMP. The MIBs supported by the relevant device must be made available to the SNMP management tools.

On the one hand, these are globally valid MIBs, which are specified and described in RFCs (Request for Comments). This includes, for example, MIB2 according to RFC1213, which is supported by all SNMP-compatible network devices. On the other hand, manufacturers can specify their own private SNMP objects, which are then assigned to a private manufacturer area in the large SNMP object tree. Manufacturers are then responsible for their own private (enterprise) areas, i.e., they must ensure that only one object is assigned to an object ID (object name and parameters) and can be published. If an object is no longer needed, it can be labeled as "expired", but it cannot be reused with other parameters under any circumstances.

Phoenix Contact provides notification of ASN1 SNMP objects by publishing their descriptions on the Internet.

Reading SNMP objects is not password-protected. However, a password is required for read access in SNMP, but this is set to "public", which is usual for network devices, and cannot be modified. By default upon delivery, the password for write access is "private" and can be changed by the user.

SNMP, the web interface, Telnet, and the serial terminal all use the same password, which can be changed by the user.

Another benefit for the user is the option of sending traps using the Simple Network Management Protocol.

Management Information Base (MIB)

Database, which contains all the data (objects and variables) required for network management.

Agent

An agent is a software tool, which collects data from the network device on which it is installed, and transmits this data on request. Agents reside in all managed network components and transmit the values of specific settings and parameters to the management station. On a request from a manager or on a specific event, the agent transmits the collected information to the management station.

Traps

Traps are spontaneous SNMP alarm or information messages, which are sent by an SNMP-compatible device when specific events occur. Traps are transmitted with maximum priority to various addresses (if required) and can then be displayed by the management station in plain text. The IP addresses that are to receive these traps (trap targets/receivers) must be set by the user on the relevant device.

trapPasswdAccess

OID	1.3.6.1.4.1.4346.11.11.3.0.1
Description	Sent to the defined trap receiver on each modification or attempted modification of the device password and contains information about the status of the last modification or attempted modification.

trapFWHealth

OID	1.3.6.1.4.1.4346.11.11.3.0.2
Description	Sent on each firmware-related modification to the diagnostic display and contains additional information about the firmware status.

trapFWConf

OID	1.3.6.1.4.1.4346.11.11.3.0.3
Description	Sent each time the configuration is saved and informs the management station that the configuration has been saved successfully. This trap is sent in the event of configuration modifications (port name, port mode, device name, IP address, trap receiver address, port mirroring, etc.), which are not yet saved permanently. The trap also provides a warning that, if not saved permanently, the modifications will be lost on a reset.

trapPowerSupply

OID	1.3.6.1.4.1.4346.11.11.3.0.4
Description	Sent each time the redundant voltage supply fails.

trapSecurityPort

OID	1.3.6.1.4.1.4346.11.11.3.0.5
Description	Sent each time a disabled MAC address accesses a port.

trapRstpRingFailure

OID	1.3.6.1.4.1.4346.11.11.3.0.6
Description	Sent in the event of a link interrupt in the redundant RSTP ring.

trapPofScrjPort

OID	1.3.6.1.4.1.4346.11.11.3.0.7
Description	Sent each time the status of the POF-SCRJ port changes.

trapPoEPort

OID	1.3.6.1.4.1.4346.11.11.3.0.8
Description	Sent each time the status of the PoE port changes.

trapManagerConnection

OID	1.3.6.1.4.1.4346.11.11.3.0.99
Description	Trap to test the connection between the SNMP agent and the network management station.

4.3.2 Diagram of SNMP Management

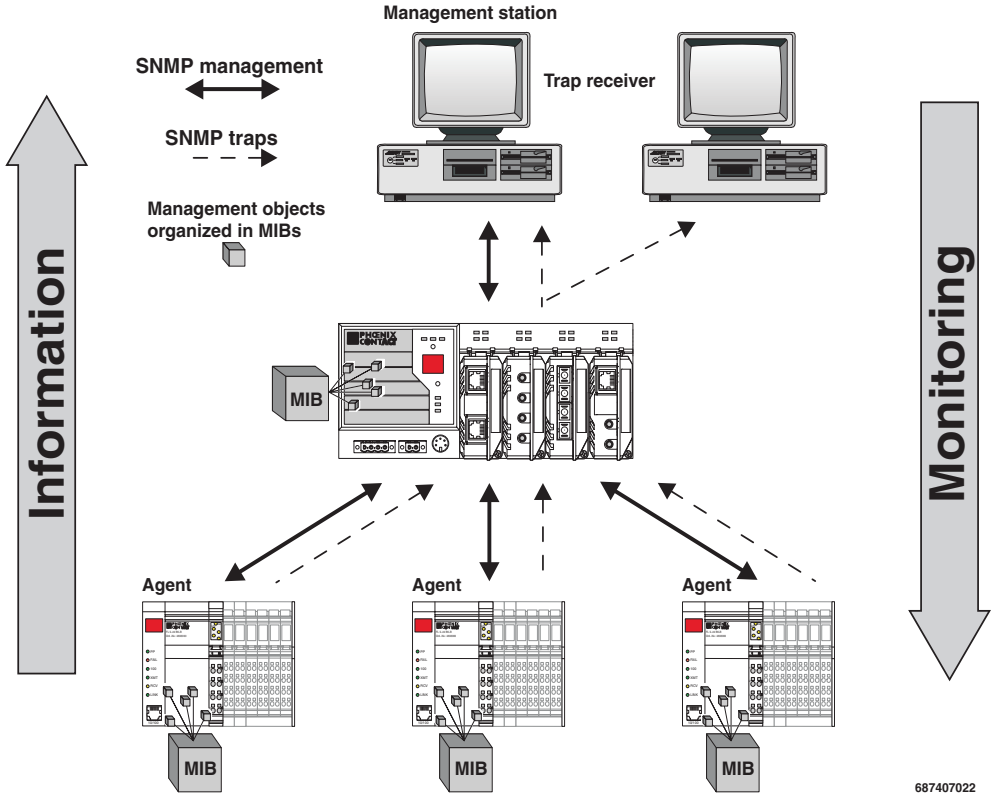


Figure 4-47 Diagram of SNMP

4.3.2.1 Tree Structure of the MIB

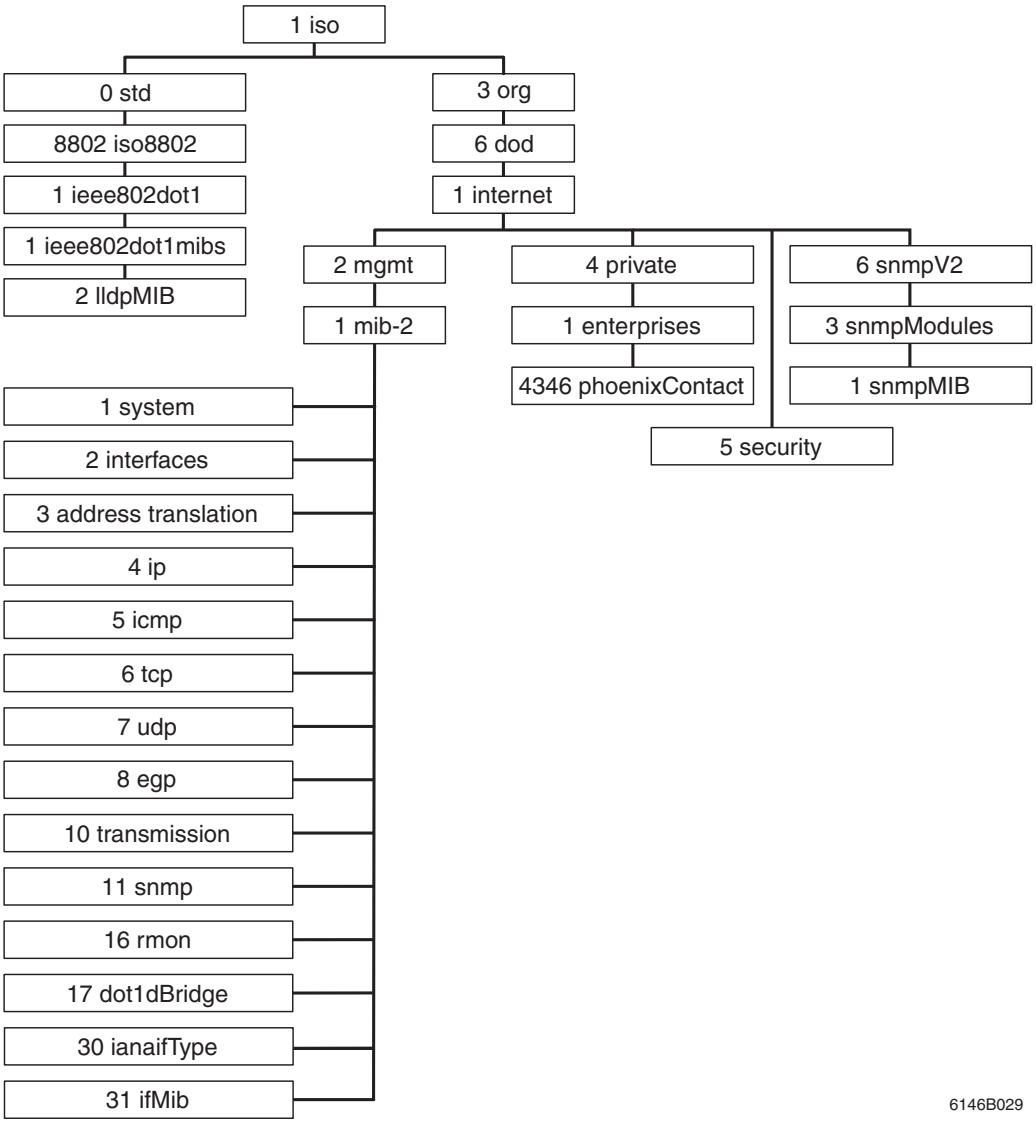


Figure 4-48 Tree structure of the MIB

Not all devices support all object classes. If an unsupported object class is requested, "not supported" is generated. If an attempt is made to modify an unsupported object class, the message "badValue" is generated.

4.3.3 RFC1213 MIB - MIB II

4.3.3.1 System Group (1.3.6.1.2.1.1)

The system group has mandatory characters for all systems. It contains system-specific objects. If an agent does not have a value for a variable, the response is a string with length 0.

(1) system

– (1) sysDescr
– (2) sysObjectID
– (3) sysUpTime
– (4) sysContact
– (5) sysName
– (6) sysLocation
– (7) sysServices
– (8) sysORLastChange
– (9) sysORTable

sysDescr

OID	1.3.6.1.2.1.1.1.0
Syntax	Octet string (size: 0 - 255)
Access	Read
Description	A textual description of the entry. The value should contain the full name and version number of: - Type of system hardware - Operation system software - Network software The description may only consist of ASCII characters that can be printed.

sysObjectID

OID	1.3.6.1.2.1.1.2.0
Syntax	Object identifier
Access	Read
Description	The authorization identification for the manufacturer of the network management subsystem, which is integrated in this device. This value is located in the SMI enterprises subtree (1.3.6.1.4.1) and describes which type of device is being managed. For example: if the manufacturer "Phoenix Contact GmbH" is assigned subtree 1.3.6.1.4.1.4346, it can then assign its bridge the identifier 1.3.6.1.4.1.4346.2.1.

sysUpTime

OID	1.3.6.1.2.1.1.3.0
Syntax	TimeTicks
Access	Read
Description	The time in hundredths of seconds since the last network management unit reset.

sysContact

OID	1.3.6.1.2.1.1.4.0
Syntax	Octet string (size: 0 - 255)
Access	Read and write
Description	The textual identification of the contact person for these managed nodes and information on how this person can be contacted.

sysName

OID	1.3.6.1.2.1.1.5.0
Syntax	Octet string (size: 0 - 255)
Access	Read and write
Description	A name for this node assigned by the administrator. According to the agreement, this is the fully qualifying name in the domain.

sysLocation

OID	1.3.6.1.2.1.1.6.0
Syntax	Octet string (size: 0 - 255)
Access	Read and write
Description	The physical location of this node (e.g., "Hall 1, 3rd floor").

sysServices

OID	1.3.6.1.2.1.1.7.0
Syntax	Integer (0 - 127)
Access	Read
Description	Indicates a number of services that this device offers. The value is the sum of several calculations. For every layer of the OSI reference model, there is a calculation in the form of (2^{L-1}), where L indicates the layer. For example: A node, which primarily executes line routing functions has the value $(2^{3-1}) = 4$. A node, which is a host and provides application services, has the value $(2^{4-1}) + (2^{7-1}) = 72$.

sysORLastChange

OID	1.3.6.1.2.1.1.8
Syntax	TimeTicks
Access	Read
Description	Indicates the value of the sysUpTime during the last system modification.

sysORTable

OID	1.3.6.1.2.1.1.9
Syntax	TimeTicks
Access	Read
Description	This table contains objects: sysORIndex, sysORID, sysORDescr, and sysORUpTime.

4.3.3.2 Interface Group (1.3.6.1.2.1.2)

The interface group contains information about device interfaces.

(2) interfaces
-- (1) ifNumber
-- (2) ifTable
-- (1) if Entry
-- (1) ifIndex
-- (2) ifDescr
-- (3) ifType
-- (4) ifMtu
-- (5) ifSpeed
-- (6) ifPhysAddress
-- (7) ifAdminStatus
-- (8) ifOperStatus
-- (9) ifLastChange
-- (10) ifInOctets
-- (11) ifInUcastPkts
-- (12) ifInNUcastPkts
-- (13) ifInDiscards
-- (14) ifInErrors
-- (15) ifInUnknownProtos
-- (16) ifOutOctets
-- (17) ifOutUcastPkts
-- (18) ifOutNUcastPkts
-- (19) ifOutDiscards
-- (20) ifOutErrors
-- (21) ifOutQLen
-- (22) ifSpecific

4.3.3.3 Address Translation Group (1.3.6.1.2.1.3)

The address translation group has mandatory characters for all systems. It contains information about the address assignment.

(3) at
-- (1) atTable
-- (1) atEntry
-- (1) atIfIndex
-- (2) atPhysAddress
-- (3) atNetAddress

4.3.3.4 Internet Protocol Group (1.3.6.1.2.1.4)

The Internet protocol group has mandatory characters for all systems. It contains information concerning IP switching.

(4) ip
-- (1) ipForwarding
-- (2) ipDefaultTTL
-- (3) ipInReceives
-- (4) ipInHdrErrors
-- (5) ipInAddrErrors
-- (6) ipForwDatagrams
-- (7) ipInUnknownProtos
-- (8) ipInDiscards
-- (9) ipInDelivers
-- (10) ipOutRequests
-- (11) ipOutDiscards
-- (12) ipOutNoRoutes
-- (13) ipReasmTimeout
-- (14) ipReasmReqds
-- (15) ipReasmOKs
-- (16) ipReasmFails
-- (17) ipFragOKs
-- (18) ipFragFails
-- (19) ipFragCreates
-- (20) ipAddrTable
-- (1) ipAddrEntry
-- (1) ipAdEntAddr
-- (2) ipAdEntIfIndex
-- (3) ipAdEntNetMask
-- (4) ipAdEntBcastAddr
-- (5) ipAdEntReasmMaxSize
-- (21) ipRouteTable
-- (1) ipRouteEntry
-- (1) ipRouteDest
-- (2) ipRouteIfIndex
-- (3) ipRouteMetric1
-- (4) ipRouteMetric2
-- (5) ipRouteMetric3
-- (6) ipRouteMetric4
-- (7) ipRouteNextHop
-- (8) ipRouteType
-- (9) ipRouteProto
-- (10) ipRouteAge
-- (11) ipRouteMask
-- (12) ipRouteMetric5
-- (13) ipRouteInfo
-- (22) ipNetToMediaTable
-- (1) ipNetToMediaEntry

-- (1) ipNetToMediaIfIndex
-- (2) ipNetToMediaPhysAddress
-- (3) ipNetToMediaNetAddress
-- (4) ipNetToMediaType
-- (23) ipRoutingDiscards

4.3.3.5 ICMP Group (1.3.6.1.2.1.5)

The Internet Control Message Protocol group has mandatory characters for all systems. It contains information about troubleshooting and control in Internet data traffic.

(5) icmp
-- (1) icmpInMsgs
-- (2) icmpInErrors
-- (3) icmpInDestUnreachs
-- (4) icmpInTimeExcds
-- (5) icmpInParmProbs
-- (6) icmpInSrcQuenchs
-- (7) icmpInRedirects
-- (8) icmpInEchos
-- (9) icmpInEchoReps
-- (10) icmpInTimestamps
-- (11) icmpInTimestampReps
-- (12) icmpInAddrMasks
-- (13) icmpInAddrMaskReps
-- (14) icmpOutMsgs
-- (15) icmpOutErrors
-- (16) icmpOutDestUnreachs
-- (17) icmpOutTimeExcds
-- (18) icmpOutParmProbs
-- (19) icmpOutSrcQuenchs
-- (20) icmpOutRedirects
-- (21) icmpOutEchos
-- (22) icmpOutEchoReps
-- (23) icmpOutTimestamps
-- (24) icmpOutTimestampReps
-- (25) icmpOutAddrMasks
-- (26) icmpOutAddrMaskReps

4.3.3.6 Transfer Control Protocol Group (1.3.6.1.2.1.6)

The Transfer Control Protocol group has mandatory characters for all systems with implemented TCP. Instances of objects, which provide information about a specific TCP connection, are valid as long as the connection is established.

(6) tcp
-- (1) tcpRtoAlgorithm
-- (2) tcpRtoMin
-- (3) tcpRtoMax
-- (4) tcpMaxConn
-- (5) tcpActiveOpens
-- (6) tcpPassiveOpens
-- (7) tcpAttemptFails
-- (8) tcpEstabResets
-- (9) tcpCurrEstab
-- (10) tcpInSegs
-- (11) tcpOutSegs
-- (12) tcpRetransSegs
-- (13) tcpConnTable
-- (1) tcpConnEntry
-- (1) tcpConnState
-- (2) tcpConnLocalAddress
-- (3) tcpConnLocalPort
-- (4) tcpConnRemAddress
-- (5) tcpConnRemPort
-- (14) tcpInErrs
-- (15) tcpOutRsts

4.3.3.7 User Datagram Protocol Group (1.3.6.1.2.1.7)

The User Datagram Protocol group has mandatory characters for all systems that implement UDP.

(7) udp
-- (1) udpInDatagrams
-- (2) udpNoPorts
-- (3) udpInErrors
-- (4) udpOutDatagrams
-- (5) udpTable
-- (1) udpEntry
-- (1) udpLocalAddress
-- (2) udpLocalPort

4.3.3.8 egp Group (1.3.6.1.2.1.8)

(8) egp
-- (1) egpInMsgs
-- (2) egpInErrors
-- (3) egpOutMsgs
-- (4) egpOutErrors
-- (5) egpNeighTable
-- (1) egpNeighEntry
-- (1) egpNeighState
-- (2) egpNeighAddr
-- (3) egpNeighAs
-- (4) egpNeighInMsgs
-- (5) egpNeighInErrs
-- (6) egpNeighOutMsgs
-- (7) egpNeighOutErrs
-- (8) egpNeighInErrMsgs
-- (9) egpNeighOutErrMsgs
-- (10) egpNeighStateUps
-- (11) egpNeighStateDowns
-- (12) egpNeighIntervalHello
-- (13) egpNeighIntervallPoll
-- (14) egpNeighMode
-- (15) egpNeighEventTrigger
-- (6) egpAs

4.3.3.9 Transmission Group (1.3.6.1.2.1.10)

(10) transmission

4.3.3.10 Simple Network Management Protocol Group (1.3.6.1.2.1.11)

The Simple Network Management Protocol group has mandatory characters for all systems. In SNMP devices, which are optimized to support either a single agent or a single management station, some of the listed objects will be overwritten with the value "0".

(11) snmp
-- (1) snmpInPkts
-- (2) snmpOutPkts
-- (3) snmpInBadVersions
-- (4) snmpInBadCommunityName
-- (5) snmpInBadCommunityUses
-- (6) snmpInASNParseErrs
-- (8) snmpInTooBigs
-- (9) snmpInNoSuchNames
-- (10) snmpInBadValues
-- (11) snmpInReadOnlys
-- (12) snmpInGenErrs
-- (13) snmpInTotalReqVars
-- (14) snmpInTotalSetVars
-- (15) snmpInGetRequests
-- (16) snmpInGetNexts

-- (17) snmpInSetRequests
-- (18) snmpInGetResponses
-- (19) snmpInTraps
-- (20) snmpOutTooBigs
-- (21) snmpOutNoSuchNames
-- (22) snmpOutBadValues
-- (24) snmpOutGenErrs
-- (25) snmpOutGetRequests
-- (26) snmpOutGetNexts
-- (27) snmpOutSetRequests
-- (28) snmpOutGetResponses
-- (29) snmpOutTraps
-- (30) snmpEnableAuthenTraps
-- (31) snmpSilentDrops
-- (32) snmpProxyDrops

4.3.4 RMON MIB (1.3.6.1.2.1.16)

This part of the MIB continuously provides the network management with up-to-date and historical network component data. The configuration of alarms and events controls the evaluation of network component counters. Depending on the configuration, the result of the evaluation is indicated to the management station by the agents using traps. The following groups are supported:

– statistics
– history
– alarm
– hosts
– hostTopN
– matrix
– filter
– capture and event

4.3.4.1 statistics (1.3.6.1.2.1.16.1)

This MIB group contains information about, e.g., the number of unicast, multicast or broadcast telegrams, telegram rate and distribution or the number of faulty telegrams classed according to error type.

The statistics group contains information about the network load and quality.

(1) etherStatsTable
-- (1) etherStatsEntry
-- (1) etherStatsIndex
-- (2) etherStatsDataSource
-- (3) etherStatsDropEvents
-- (4) etherStatsOctets
-- (5) etherStatsPkts
-- (6) etherStatsBroadcastPkts
-- (7) etherStatsMulticastPkts
-- (8) etherStatsCRCAlignErrors
-- (9) etherStatsUndersizePkts
-- (10) etherStatsOversizePkts
-- (11) etherStatsFragments
-- (12) etherStatsJabbers
-- (13) etherStatsCollisions
-- (14) etherStatsPkts64Octets
-- (15) etherStatsPkts65to127Octets
-- (16) etherStatsPkts128to255Octets
-- (17) etherStatsPkts256to511Octets
-- (18) etherStatsPkts512to1023Octets
-- (19) etherStatsPkts1024to1518Octets
-- (20) etherStatsOwner
-- (21) etherStatsStatus

4.3.4.2 history (1.3.6.1.2.1.16.2)

The history group contains statistical information, which can be read and represented, e.g., as a time curve.

(1) historyControlTable
-- (1) historyControlEntry
-- (1) historyControlIndex
-- (2) historyControlDataSource
-- (3) historyControlBucketsRequested
-- (4) historyControlBucketsGranted
-- (5) historyControlInterval
-- (6) historyControlOwner
-- (7) historyControlStatus
(2) etherhistoryTable
-- (1) etherhistoryEntry
-- (1) etherHistoryIndex
-- (2) etherHistorySampleIndex
-- (3) etherHistoryIntervalStart
-- (4) etherHistoryDropEvents
-- (5) etherHistoryOctets

-- (6) etherHistoryPkts
-- (7) etherHistoryBroadcastPkts
-- (8) etherHistoryMulticastPkts
-- (9) etherHistoryCRCAlignErrors
-- (10) etherHistoryUndersizePkts
-- (11) etherHistoryOversizePkts
-- (12) etherHistoryFragments
-- (13) etherHistoryJabbers
-- (14) etherHistoryCollisions
-- (15) etherHistoryUtilization

4.3.4.3 alarm (1.3.6.1.2.1.16.3)

The alarm group requests statistical values and compares them with the defined limit values. If a value is above or below the limit value, an alarm and a trap are generated.

(1) alarmTable
-- (1) alarmEntry
-- (1) alarmIndex
-- (2) alarmInterval
-- (3) alarmVariable
-- (4) alarmSampleType
-- (5) alarmValue
-- (6) alarmStartupAlarm
-- (7) alarmRisingThreshold
-- (8) alarmFallingThreshold
-- (9) alarmRisingEventIndex
-- (10) alarmFallingEventIndex
-- (11) alarmOwner
-- (12) alarmStatus

4.3.4.4 hosts (1.3.6.1.2.1.16.4)

(1) hostControlTable
-- (1) hostControlEntry
-- (1) hostControlIndex
-- (2) hostControlDataSource
-- (3) hostControlTableSize
-- (4) hostControlLastDeleteTime
-- (5) hostControlOwner
-- (6) hostControlStatus
-- (2) hostTable
-- (1) hostEntry
-- (1) hostAddress
-- (2) hostCreationOrder
-- (3) hostIndex
-- (4) hostInPkts
-- (5) hostOutPkts
-- (6) hostInOctets
-- (7) hostOutOctets
-- (8) hostOutErrors

-- (9) hostOutBroadcastPkts
-- (10) hostOutMulticastPkts
-- (3) hostTimeTable
-- (1) hostTimeEntry
-- (1) hostTimeAddress
-- (2) hostTimeCreationOrder
-- (3) hostTimeIndex
-- (4) hostTimeInPkts
-- (5) hostTimeOutPkts
-- (6) hostTimeInOctets
-- (7) hostTimeOutOctets
-- (8) hostTimeOutErrors
-- (9) hostTimeOutBroadcastPkts
-- (10) hostTimeOutMulticastPkts

4.3.4.5 hostTopN (1.3.6.1.2.1.16.5)

(1) hostTopNControlTable
-- (1) hostTopNControlEntry
-- (1) hostTopNControlIndex
-- (2) hostTopNHostINdex
-- (3) hostTopNRateBase
-- (4) hostTopNTimeRemaining
-- (5) hostTopNDuration
-- (6) hostTopNRequestedSize
-- (7) hostTopNGrantedSize
-- (8) hostTopNStartTime
-- (9) hostTopNOwner
-- (10) hostTopNStatus
-- (2) hostTopNTable
-- (1) hostTopNEntry
-- (1) hostTopNReport
-- (2) hostTopNIndex
-- (3) hostTopNAddress
-- (4) hostTopNRate

4.3.4.6 matrix (1.3.6.1.2.1.16.6)

-- (1) martrixControlTable
-- (1) matrixControlEntry
-- (1) matrixControlIndex
-- (2) matrixControlDataSource
-- (3) matrixControlTableSize
-- (4) matrixControlLastDeleteTime
-- (5) matrixControlOwner
-- (6) matrixControlStatus
-- (2) matrixSDTable
-- (1) matrixSDEntry
-- (1) matrixSDSourceAddress
-- (2) matrixSDDestAddress

-- (3) matrixSDIndex
-- (4) matrixSDPkts
-- (5) matrixSDOctets
-- (6) matrixSDErrors
-- (3) matrixDSTable
-- (1) matrixDSEntry
-- (1) matrixDSSourceAddress
-- (2) matrixDSDestAddress
-- (3) matrixDSIndex
-- (4) matrixDSPkts
-- (5) matrixDSOctets
-- (6) matrixDSErrors

4.3.4.7 filter (1.3.6.1.2.1.16.7)

(1) filterTable
-- (1) filterEntry
-- (1) filterIndex
-- (2) filterChannelIndex
-- (3) filterPktDataOffset
-- (4) filterPktData
-- (5) filterPktDataMask
-- (6) filterPktDataNotMask
-- (7) filterPktStatus
-- (8) filterPktStatusMask
-- (9) filterPktStatusNotMask
-- (10) filterOwner
-- (11) filterStatus
(2) channelTable
-- (1) channelEntry
-- (1) channelIndex
-- (2) channelIfIndex
-- (3) channelAcceptTime
-- (4) channelDataControl
-- (5) channelTurnOnEventIndex
-- (6) channelTurnOffEventIndex
-- (7) channelEventIndex
-- (8) channelEventStatus
-- (9) channelMatches
-- (10) channelDescription
-- (11) channelOwner
-- (12) channelStatus

4.3.4.8 capture (1.3.6.1.2.1.16.8)

(1) bufferControlTable
-- (1) bufferControlEntry
-- (1) bufferControlIndex
-- (2) bufferControlChannelIndex
-- (3) bufferControlFullStatus
-- (4) bufferControlFullAction
-- (5) bufferControlCaptureSliceSize
-- (6) bufferControlDownloadSliceSize
-- (7) bufferControlDownloadOffset
-- (8) bufferControlMaxOctetsRequested
-- (9) bufferControlMaxOctetsGranted
-- (10) bufferControlCapturedPackets
-- (11) bufferControlTurnOnTime
-- (12) bufferControlOwner
-- (13) bufferControlStatus
(2) captureBufferTable
-- (1)captureBufferEntry
-- (1)captureBufferControlIndex
-- (2)captureBufferIndex
-- (3) captureBufferPacketID
-- (4) captureBufferPacketData
-- (5) captureBufferPacketLength
-- (6) captureBufferPacketTime
-- (7) captureBufferPacketStatus

4.3.4.9 event (1.3.6.1.2.1.16.9)

The event group controls the generation of traps when the alarms described above occur.

(1) eventTable
-- (1) eventEntry
-- (1) eventIndex
-- (2) eventDescription
-- (3) eventType
-- (4) eventCommunity
-- (5) eventLastTimeSent
-- (6) eventOwner
-- (7) eventStatus
(2) logTable
-- (1) logEntry
-- (1) logEventIndex
-- (2) logIndex
-- (3) logTime
-- (4) logDescription

4.3.5 Bridge MIB (1.3.6.1.2.1.17)

4.3.5.1 dot1dBase (1.3.6.1.2.1.17.1)

The dot1dBase group contains bridge-specific information.

(1) dot1dBaseBridgeAddress
(2) dot1dBaseNumPorts
(3) dot1dBasePortType
(4) dot1dBasePortTable
-- dot1dBasePortEntry
-- (1) dot1dBasePort
-- (2) dot1dBasePortIfIndex
-- (3) dot1dBasePortPortCircuit
-- (4) dot1dBasePortDelayExceededDiscards
-- (5) dot1dBasePortMtuExceededDiscards

4.3.5.2 dot1dStp (1.3.6.1.2.1.17.2)

-- (1) dot1dStpProtocolSpecification
-- (2) dot1dStpPriority
-- (3) dot1dStpTimeSinceTopologyChange
-- (4) dot1dStpTopChanges
-- (5) dot1dStpDesignateRoot
-- (6) dot1dStpRootCost
-- (7) dot1dStpRootPort
-- (8) dot1dStpMaxAge
-- (9) dot1dStpHelloTime
-- (10) dot1dStpHoldTime
-- (11) dot1dStpForwardDelay
-- (12) dot1dStpBridgeMaxAge
-- (13) dot1dStpBridgeHelloTime
-- (14) dot1dStpBridgeForwardDelay
-- (15) dot1dStpPortTable
-- (1) dot1dStpPortEntry
-- (1) dot1dStpPort
-- (2) dot1dStpPortPriority
-- (3) dot1dStpPortState
-- (4) dot1dStpPortEnable
-- (5) dot1dStpPortPathCost
-- (6) dot1dStpPortDesignatedRoot
-- (7) dot1dStpPortDesignatedCost
-- (8) dot1dStpPortDesignatedBridge
-- (9) dot1dStpPortDesignatedPort
-- (10) dot1dStpPortForwardTransitions
-- (11) dot1dStpPortPathCost32
-- (16) dot1dStpVersion
-- (17) dot1dStpTxHoldCount
-- (18) dot1dStpPathCostDefault
-- (19) dot1dStpExtPortTable

-- (1) dot1dStpExtPortEntry
-- (1) dot1dStpPortProtocolMigration
-- (2) dot1dStpPortAdminEdgePort
-- (3) dot1dStpPortOperEdgePort
-- (4) dot1dStpPortAdminPointToPoint
-- (5) dot1dStpPortOperPointToPoint
-- (6) dot1dStpPortAdminPathCost

4.3.5.3 dot1dTp (1.3.6.1.2.1.17.4)

The dot1dTp group contains bridge-specific information.

(1) dot1dTpLearnedEntryDiscards
(2) dot1dTpAgingTime
(3) dot1dTpFdbTable
-- (1) dot1dTpFdbEntry
-- (1) dot1dTpFdbAddress
-- (2) dot1dTpFdbPort
-- (3) dot1dTpFdbStatus
(4) dot1dTpPortTable
-- dot1dTpPortEntry
-- (1) dot1dTpPort
-- (2) dot1dTpPortMaxInfo
-- (3) dot1dTpPortInFrames
-- (4) dot1dTpPortOutFrames
-- (5) dot1dTpPortInDiscards
(5) dot1dTpHCPortTable
-- dot1dTpHCPortEntry
-- (1) dot1dTpHCPortInFrames
-- (2) dot1dTpHCPortOutFrames
-- (3) dot1dTpHCPortInDiscards
(6) dot1dTpPortOverflowTable
-- dot1dTpPortOverflowEntry
-- (1) dot1dTpPortInOverflowFrames
-- (2) dot1dTpPortOutOverflowFrames
-- (3) dot1dTpPortInOverflowDiscards

4.3.5.4 dot1dStatic (1.3.6.1.2.1.17.5)

-- (1) dot1dStaticTable
-- (1) dot1dStaticEntry
-- (1) dot1dStaticAddress
-- (2) dot1dStaticReceivePort
-- (3) dot1dStaticAllowedToGoTo

4.3.6 pBridgeMIB (1.3.6.1.2.1.17.6)

4.3.6.1 pBridgeMIBObjects (1.3.6.1.2.1.17.6.1)

-- (1) dot1dExtBase
- -- (1) dot1dDeviceCapabilities
- -- (2) dot1dTrafficClassesEnabled
- -- (3) dot1dGmrpStatus
- -- (4) dot1dCapabilitiesTable
  - -- (1) dot1dCapabilitiesEntry
  - -- (1) dot1dPortCapabilities

-- (2) dot1dPriority
- -- (1) dot1dPortPriorityTable
  - -- (1) dot1dPortPriorityEntry
  - -- (1) dot1dPortDefaultUserPriority
  - -- (2) dot1dPortNumTrafficClasses
- -- (2) dot1dUserPriorityRegenTable
  - -- (1) dot1dUserPriorityRegenTable
  - -- (1) dot1dUserPriority
  - -- (2) dot1dRegenUserPriority
- -- (3) dot1dTrafficClassTable
  - -- (1) dot1dTrafficClassEntry
  - -- (1) dot1dTrafficClassPriority
  - -- (2) dot1dTrafficClass
- -- (4) dot1dPortOutboundAccessPriorityTable
  - -- (1) dot1dPortOutboundAccessPriorityEntry
  - -- (1) dot1dPortOutboundAccessPriority

-- (3) dot1dGarp
- -- (1) dot1dPortGarpTable
  - -- (1) dot1dPortGarpEntry
  - -- (1) dot1dPortGarpJoinTime
  - -- (2) dot1dPortGarpLeaveTime
  - -- (3) dot1dPortGarpLeaveAllTime

-- (4) dot1dGmrp
- -- (1) dot1dPortGmrpTable
  - -- (1) dot1dPortGmrpEntry
  - -- (1) dot1dPortGmrpStatus
  - -- (2) dot1dPortGmrpFailedRegistrations
  - -- (3) dot1dPortGmrpLastPduOrigin

4.3.6.2 pBridgeConformance (1.3.6.1.2.1.17.6.2)

-- (1) pBridgeGroups
- -- (1) pBridgeExtCapGroup
- -- (2) pBridgeDeviceGmrpGroup
- -- (3) pBridgeDevicePriorityGroup
- -- (4) pBridgeDefaultPriorityGroup
- -- (5) pBridgeRegentPriorityGroup
- -- (6) pBridgePriorityGroup
- -- (7) pBridgeAccessPriorityGroup

-- (8) pBridgePortGarpGroup
-- (9) pBridgePortGmrpGroup
-- (10) pBridgeHCPortGroup
-- (11) pBridgePortOverflowGroup
-- (2) pBridgeCompliances
-- (1) pBridgeCompliance

4.3.7 qBridgeMIB (1.3.6.1.2.1.17.7)

4.3.7.1 qBridgeMIBObjects (1.3.6.1.2.1.17.7.1)

-- (1) dot1qBase
-- (1) dot1qVLANVersionNumber
-- (2) dot1qMaxVLANId
-- (3) dot1qMaxSupportedVLANs
-- (4) dot1qNumVLANs
-- (5) dot1qGvrpStatus
-- (2) dot1qTp
-- (1) dot1qFdbTable
-- (1) dot1qFdbEntry
-- (1) dot1qFdbId
-- (2) dot1qFdbDynamicCount
-- (2) dot1qTpFdbTable
-- (1) dot1qTpFdbEntry
-- (1) dot1qTpFdbAddress
-- (2) dot1qTpFdbPort
-- (3) dot1qTpFdbStatus
-- (3) dot1qTpGroupTable
-- (1) dot1qTpGroupEntry
-- (1) dot1qTpGroupAddress
-- (2) dot1qTpGroupEgressPorts
-- (3) dot1qTpGroupLearnt
-- (4) dot1qForwardAllTable
-- (1) dot1qForwardAllEntry
-- (1) dot1qForwardAllPorts
-- (2) dot1qForwardAllStaticPorts
-- (3) dot1qForwardAllForbiddenPorts
-- (5) dot1qForwardUnregisteredTable
-- (1) dot1qForwardUnregisteredEntry
-- (1) dot1qForwardUnregisteredPorts
-- (2) dot1qForwardUnregisteredStaticPorts
-- (3) dot1qForwardUnregisteredForbiddenPorts
-- (3) dot1qStatic
-- (1) dot1qStaticUnicastTable
-- (1) dot1qStaticUnicastEntry
-- (1) dot1qStaticUnicastAddress
-- (2) dot1qStaticUnicastReceivePort
-- (3) dot1qStaticUnicastAllowedToGoTo
-- (4) dot1qStaticUnicastStatus

-- (2) dot1qStaticMulticastTable
-- (1) dot1qStaticMulticastEntry
-- (1) dot1qStaticMulticastAddress
-- (2) dot1qStaticMulticastReceivePort
-- (3) dot1qStaticMulticastStaticEgressPorts
-- (4) dot1qStaticMulticastForbiddenEgressPorts
-- (5) dot1qStaticMulticastStatus
-- (4) dot1qVLAN
-- (1) dot1qVLANNumDeletes
-- (2) dot1qVLANCurrentTable
-- (1) dot1qVLANCurrentEntry
-- (1) dot1qVLANTimeMark
-- (2) dot1qVLANIndex
-- (3) dot1qVLANFdbId
-- (4) dot1qVLANCurrentEgressPorts
-- (5) dot1qVLANCurrentUntaggedPorts
-- (6) dot1qVLANStatus
-- (7) dot1qVLANCreationTime
-- (3) dot1qVLANStaticTable
-- (1) dot1qVLANStaticEntry
-- (1) dot1qVLANStaticName
-- (2) dot1qVLANStaticEgressPorts
-- (3) dot1qVLANForbiddenEgressPorts
-- (4) dot1qVLANStaticUntaggedPorts
-- (5) dot1qVLANStaticRowStatus
-- (4) dot1qNextFreeLocalVLANIndex
-- (5) dot1qPortVLANTable
-- (1) dot1qPortVLANEntry
-- (1) dot1qPvid
-- (2) dot1qPortAcceptableFrameTypes
-- (3) dot1qPortIngressFiltering
-- (4) dot1qPortGvrpStatus
-- (5) dot1qPortGvrpFailedRegistrations
-- (6) dot1qPortGvrpLastPduOrigin
-- (6) dot1qPortVLANStatisticsTable
-- (1) dot1qPortVLANStatisticsEntry
-- (1) dot1qTpVLANPortInFrames
-- (2) dot1qTpVLANPortOutFrames
-- (3) dot1qTpVLANPortInDiscards
-- (4) dot1qTpVLANPortInOverflowFrames
-- (5) dot1qTpVLANPortOutOverflowFrames
-- (6) dot1qTpVLANPortInOverflowDiscards
-- (7) dot1qPortVLANHCStatisticsTable
-- (1) dot1qPortVLANHCStatisticsEntry
-- (1) dot1qPortVLANHCInFrames
-- (2) dot1qPortVLANHCOutFrames
-- (3) dot1qPortVLANHCIn Discards
-- (8) dot1qLearningConstraintsTable
-- (1) dot1qLearningConstraintsEntry
-- (1) dot1qConstraintVLAN

-- (2) dot1qConstraintSet
-- (3) dot1qConstraintType
-- (4) dot1qConstraintStatus
-- (9) dot1qConstraintSetDefault
-- (10) dot1qConstraintTypeDefault

4.3.7.2 qBridgeConformance (1.3.6.1.2.1.17.7.2)

-- (1) qBridgeGroups
-- (1) qBridgeBaseGroup
-- (2) qBridgeFdbUnicastGroup
-- (3) qBridgeFdbMulticastGroup
-- (4) qBridgeServiceRequirementsGroup
-- (5) qBridgeFdbStaticGroup
-- (6) qBridgeVLANGroup
-- (7) qBridgeVLANStaticGroup
-- (8) qBridgePortGroup
-- (9) qBridgeVLANStatisticsGroup
-- (10) qBridgeVLANStatisticsOverflowGroup
-- (11) qBridgeVLANHCStatisticsGroup
-- (12) qBridgeLearningConstraintsGroup
-- (13) qBridgeLearningConstraintDefaultGroup
-- (2) qBridgeCompliances
-- (1) qBridgeCompliance

4.3.7.3 dot1dConformance (1.3.6.1.2.1.17.7.3)

-- (1) dot1dGroups
-- (1) dot1dBaseBridgeGroup
-- (2) dot1BasePortGroup
-- (3) dot1dStpBridgeGroup
-- (4) dot1dStpPortGroup2
-- (5) dot1dStpPortGroup3
-- (6) dot1dTpBridgeGroup
-- (7) dot1dTpSdbGroup
-- (8) dot1dTpGroup
-- (9) dot1dStaticGroup
-- (10) dot1dNotificationGroup
-- (2) dot1dCompliances
-- (1) BridgeCompliances1493
-- (2) BridgeCompliances4188

4.3.8 rstp MIB (1.3.6.1.2.1.17.11)

4.3.8.1 rstp Conformance (1.3.6.1.2.1.17.11.1)

rstp Groups (1.3.6.1.2.1.17.11.1.1)

-- (1) rstpBridgeGroups
-- (2) rstpDefaultPathCostGroup
-- (3) rstpPortGroup

rstp Compliance Groups (1.3.6.1.2.1.17.11.1.2)

-- (1) rstpCompliance

4.3.9 IANAifType MIB (1.3.6.1.2.1.30)

The IANAifType MIB defines the "ifTable" in MIB II. See "Interface Group (1.3.6.1.2.1.2)" on page 4-47.

4.3.10 IF MIB (1.3.6.1.2.1.31)

4.3.10.1 ifMIBObjects (1.3.6.1.2.1.31.1)

-- (1) ifXTable
  -- (1) ifXEntry
    -- (1) ifName
    -- (2) ifInMulticastPkts
    -- (3) ifInBroadcastPkts
    -- (4) ifOutMulticastPkts
    -- (5) ifOutBroadcastPkts
    -- (6) ifHCInOctets
    -- (7) ifHCInUcastPkts
    -- (8) ifHCInMulticastPkts
    -- (9) ifHCInBroadcastPkts
    -- (10) ifHCOutOctets
    -- (11) ifHCOutUcastPkts
    -- (12) ifHCOutMulticastPkts
    -- (13) ifHCOutBroadcastPkts
    -- (14) ifLinkUpDownTrapEnable
    -- (15) ifHighSpeed
    -- (16) ifPromiscuousMode
    -- (17) ifConnectorPresent
    -- (18) ifAlias
    -- (19) ifCounterDiscontinuityTime
-- (2) ifStackTable
  -- (1) ifStackEntry
    -- (1) ifStackHigherLayer
    -- (2) ifStackLowerLayer

-- (3) ifStackStatus
-- (3) ifTestTable
-- (1) ifTestEntry
-- (1) ifTestID
-- (2) ifTestStatus
-- (3) ifTestType
-- (4) ifTestResult
-- (5) ifTestCode
-- (6) ifTestOwner
-- (4) ifRcvAddressTable
-- (1) ifRcvAddressEntry
-- (1) ifRcvAddressAddress
-- (2) ifRcvAddressStatus
-- (3) ifRcvAddressType
-- (5) ifTableLastChange
-- (6) ifStackLastChange

4.3.10.2 ifConformance (1.3.6.1.2.1.31.2)

-- (1) ifGroups
-- (1) ifGeneralGroup
-- (2) ifFixedLengthGroup
-- (3) ifHCFixedLengthGroup
-- (4) ifPacketGroup
-- (5) ifHCPacketGroup
-- (6) ifVHCPacketGroup
-- (7) ifRcvAddressGroup
-- (8) ifTestGroup
-- (9) ifStackGroup
-- (10) ifGeneralInformationGroup
-- (11) ifStackGroup2
-- (12) ifOldObjectsGroup
-- (13) ifCounterDiscontinuityGroup
-- (2) ifCompliances
-- (1) ifCompliance
-- (2) ifCompliance2

4.3.10.3 etherMIBObjects (1.3.6.1.2.1.32.1)

-- (1) etherConformance
-- (1) etherGroups
-- (1) etherStatsGroup
-- (2) etherCollisionTableGroup
-- (3) etherStats100BbsGroup
-- (4) etherStatsBaseGroup
-- (5) etherStatsLowSpeedGroup
-- (6) etherStatsHighSpeedGroup
-- (7) etherDuplexGroup
-- (8) etherControlGroup

-- (9) etherControlPauseGroup
-- (1) etherCompliances
-- (1) etherCompliances
-- (2) ether100MbsCompliance
-- (3) dot3Compliance

4.3.10.4 lldpMIB (1.0.8802.1.1.2)

(1) lldpObjects
-- (1) lldpConfiguration
-- (1) lldpMessageTxInterval
-- (2) lldpMessageTxHoldMultiplier
-- (2) lldpStatistics
-- (3) lldpLocalSystemData
-- (1) lldpLocChassisIdSubType
-- (2) lldpLocChassisId
-- (3) lldpLocSysName
-- (4) lldpLocSysDesc
-- (5) lldpLocSysCapSupported
-- (6) lldpLocSysCapEnabled
-- (7) lldpLocPortTable
-- (1) lldpLocPortMum
-- (2) lldpLocPortIdSubtype
-- (3) lldpLocPortId
-- (4) lldpLocPortDesc
-- (8) lldpLocManAddrTable
-- (1) lldpLocManAddrSubtype
-- (2) lldpLocManAddr
-- (3) lldpLocManAddrLen
-- (4) lldpLocManAddrIfSubtype
-- (5) lldpLocManAddrIfId
-- (6) lldpLocManAddrOID
-- (4) lldpRemoteSystemsData
-- (1) lldpRemTable
-- (1) lldpRemTimeMark
-- (2) lldpRemLocalPortNum
-- (3) lldpRemIndex
-- (4) lldpRemChassisType
-- (5) lldpRemChassisId
-- (6) lldpRemPortIdSubtype
-- (7) lldpRemPortId
-- (8) lldpRemPortDesc
-- (9) lldpRemSysName
-- (10) lldpRemSysDesc
-- (11) lldpRemSysCapSupported
-- (12) lldpRemSysCapEnabled
-- (2) lldpRemManAddrTable
-- (1) lldpRemAddrSubSubtype

```
                -- (2) lldpRemManAddr
                -- (3) lldpRemManAddrIfSubtype
                -- (4) lldpRemManAddrIfId
                -- (5) lldpRemManAddrOID
        -- (5) lldpConformance
```

4.3.11 Private MIBs

The private MIBs for the MMS from Phoenix Contact can be found under object ID 1.3.6.1.4.1.4346. The MMS MIB contains the following groups:

– pxcModules (OID = 1.3.6.1.4.1.4346.1)
– pxcGlobal (OID = 1.3.6.1.4.1.4346.2)
– pxcFactoryLine (OID = 1.3.6.1.4.1.4346.11)

All configuration modifications, which are to take effect after an MMS restart, must be saved permanently using the "flWorkFWCtrlConfSave" object.

The aging time (default: 40 seconds) is not set using the private MIBs, instead it is set using the "dot1dTpAgingTime" MIB object (OID 1.3.6.1.2.1.17.4.2). The available setting range is 10 - 825 seconds.

MIB Tree

The private MIB from Phoenix Contact is integrated in the MIB tree as follows (see red arrow).

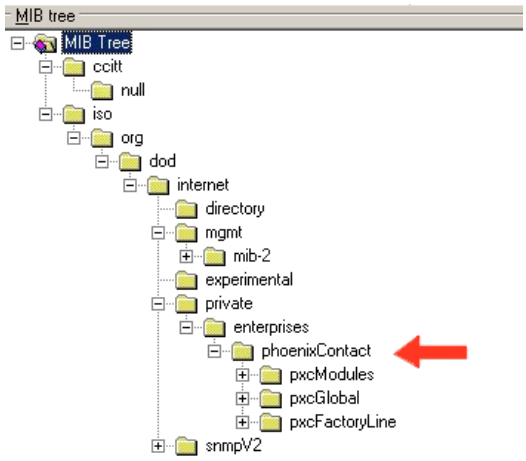


Figure 4-49 MIB tree

4.3.11.1 pxcModules OID = 1.3.6.1.4.1.4346.1

flMSwitchMModule

OID 1.3.6.1.4.1.4346.1.8

The object contains information about the manufacturer.

4.3.11.2 pxcGlobal OID = 1.3.6.1.4.1.4346.2

pxcBasic

OID 1.3.6.1.4.1.4346.2.1

	pxcBasicName
OID	1.3.6.1.4.1.4346.2.1.1
Syntax	Display string
Access	Read
Description	Contains the manufacturer's name: Phoenix Contact GmbH & Co. KG.
	pxcBasicDescr
OID	1.3.6.1.4.1.4346.2.1.2
Syntax	Display string
Access	Read
Description	Contains the manufacturer's name and address: Phoenix Contact GmbH & Co. KG P.O. Box 1341 D-32819 Blomberg.
	pxcBasicURL
OID	1.3.6.1.4.1.4346.2.1.3
Syntax	Display string
Access	Read
Description	Contains the manufacturer's web address: http://www.phoenixcontact.com.

4.3.11.3 pxcFactoryLine OID = 1.3.6.1.4.1.4346.11

	flGlobal
OID	1.3.6.1.4.1.4346.11.1
	flBasic
OID	1.3.6.1.4.1.4346.11.1.1
	flBasicName
OID	1.3.6.1.4.1.4346.11.1.1.1
Syntax	Display string
Access	Read
Description	Contains the name of the product group: Factory Line.

	flBasicDescr
OID	1.3.6.1.4.1.4346.11.1.1.2
Syntax	Display string
Access	Read
Description	Contains a brief description of the product group: Ethernet Installation System.
	flBasicURL
OID	1.3.6.1.4.1.4346.11.1.1.3
Syntax	Display string
Access	Read
Description	Contains a specific URL for the product group: www.factoryline.de.
	flBasicCompCapacity
OID	1.3.6.1.4.1.4346.11.1.1.4
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Contains the number of different components that can be managed with this device.
	flComponents
OID	1.3.6.1.4.1.4346.11.1.2
	flComponentsTable
OID	1.3.6.1.4.1.4346.11.1.2.1
	flComponentsTableEntry

OID	1.3.6.1.4.1.4346.11.1.2.1.1
Syntax	
Access	
Description	Generates a table with descriptions for components in the "Factory Line" product group, which can be managed by this management unit.
flComponentsIndex	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.1
Syntax	Integer32 (1 - 1024)
Access	Read

Description	Contains the product index for the component.
flComponentsName	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.2
Syntax	Display string
Access	Read
Description	Contains the designation of the component.
flComponentsDescr	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.3
Syntax	Display string
Access	Read
Description	Contains a brief description of the component.
flComponentsURL	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.4
Syntax	Display string
Access	Read
Description	Contains the URL of a website with additional information: www.factoryline.de.
flComponentsOrderNumber	
OID	1.3.6.1.4.1.4346.11.1.2.1.1.5
Syntax	Display string
Access	Read
Description	Contains the Order No. of the component.

flWorkDevice

OID 1.3.6.1.4.1.4346.11.11

flWorkBasic

OID 1.3.6.1.4.1.4346.11.11.1

flWorkBasicName

OID	1.3.6.1.4.1.4346.11.11.1.1
Syntax	Display string
Access	Read and write
Description	Contains the device name (corresponds to "sysName" from MIB2).

flWorkBasicDescr

OID	1.3.6.1.4.1.4346.11.11.1.2
Syntax	Display string
Access	Read and write
Description	Contains a brief description (corresponds to "sysDescr" from MIB2).

flWorkBasicURL

OID	1.3.6.1.4.1.4346.11.11.1.3
Syntax	Display string
Access	Read
Description	Contains the URL of the device-specific web page for WBM in the form of the currently set IP address.

flWorkBasicSerialNumber

OID	1.3.6.1.4.1.4346.11.11.1.4
Syntax	Octet string (12)
Access	Read
Description	Contains the serial number of the device.

flWorkBasicHWRevision

OID	1.3.6.1.4.1.4346.11.11.1.5
Syntax	Octet string (4)
Access	Read
Description	Contains the hardware version of the device.

flWorkBasicPowerStat

OID	1.3.6.1.4.1.4346.11.11.1.6
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Contains status information about the connected supply voltages: Unknown 1 Supply voltage 1 OK 3 Supply voltage 2 OK 4 Supply voltage 1 and 2 OK 5

flWorkBasicSystemBusversion

OID	1.3.6.1.4.1.4346.11.11.1.7
Syntax	Octet string (4)
Access	Read
Description	Contains the version number for the system bus.

flWorkBasicCompMaxCapacity

OID	1.3.6.1.4.1.4346.11.11.1.11
Syntax	Integer 32
Access	Read
Description	Contains the maximum number of interfaces that can be connected.

flWorkBasicCompCapacity

OID	1.3.6.1.4.1.4346.11.11.1.12
Syntax	Integer 32
Access	Read
Description	Contains the number of interfaces actually connected.

flWorkComponents

OID	1.3.6.1.4.1.4346.11.11.2

flWorkComponentsTable

OID	1.3.6.1.4.1.4346.11.11.2.1

flWorkComponentsEntry

OID	1.3.6.1.4.1.4346.11.11.2.1.1
Description	Generates a table with the available interface modules of this switch station.
flWorkComponentsIndex	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Indicates the selected interface number.
flWorkComponentsOID	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.2
Syntax	OBJECT IDENTIFIER
Access	Read
Description	This OID indicates the corresponding entry in flWorkComponentsEntry.
flWorkComponentsURL	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.3
Syntax	Display string
Access	Read
Description	Contains the IP address of the switch.
flWorkComponentsDevSign	
OID	1.3.6.1.4.1.4346.11.11.2.1.1.4
Syntax	Integer (0 - 24)
Access	Read
Description	Contains the designation of the interface module.

flWorkTraps

OID 1.3.6.1.4.1.4346.11.11.3

flWorkTrapsDelemeter

OID 1.3.6.1.4.1.4346.11.11.3.0

trapPasswdAccess

OID 1.3.6.1.4.1.4346.11.11.3.0.1

Description Sent to the defined trap receiver on each modification or attempted modification of the device password and contains information about the status of the last modification or attempted modification.

trapFWHealth

OID 1.3.6.1.4.1.4346.11.11.3.0.2

Description Sent on each firmware-related modification to the diagnostic display and contains additional information about the firmware status.

trapFWConf

OID 1.3.6.1.4.1.4346.11.11.3.0.3

Description Sent each time the configuration is saved and informs the management station that the configuration has been saved successfully.
This trap is sent in the event of configuration modifications (port name, port mode, device name, IP address, trap receiver address, port mirroring, etc.), which are not yet saved permanently. The trap also provides a warning that, if not saved permanently, the modifications will be lost on a reset.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

trapPowerSupply

OID 1.3.6.1.4.1.4346.11.11.3.0.4

Description Sent each time the redundant voltage supply fails.

trapSecurityPort

OID 1.3.6.1.4.1.4346.11.11.3.0.5

Description Sent each time a disabled MAC address accesses a port.

trapRstpRingFailure

OID 1.3.6.1.4.1.4346.11.11.3.0.6

Description Sent in the event of a link interrupt in the redundant RSTP ring.

trapPofScrjPort

OID	1.3.6.1.4.1.4346.11.11.3.0.7
Description	Sent in the event of switch-over to or from a critical state.

trapPoEPort

OID	1.3.6.1.4.1.4346.11.11.3.0.8
Description	Always sent if the error status of a PoE port changes.

trapManagerConnection

OID	1.3.6.1.4.1.4346.11.11.3.0.99
Description	This trap is used to test the connection between the device and trap manager.

flWorkNet

OID	1.3.6.1.4.1.4346.11.11.4

flWorkNetIfParameter

OID	1.3.6.1.4.1.4346.11.11.4.1

flWorkNetIfParamPhyAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.1
Syntax	MAC address
Access	Read
Description	Contains the MAC address of the switch.

flWorkNetIfParamIPAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.2
Syntax	IP address
Access	Read and write
Description	Contains the current IP address of the MMS. Modifications only take effect once the "flWorkNetIfParamSave" object has been executed.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

flWorkNetIfParamSubnetmask

OID	1.3.6.1.4.1.4346.11.11.4.1.3

Syntax	IP address
Access	Read and write
Description	Contains the current subnet mask of the MMS. Modifications only take effect once the "flWorkNetIfParamSave" object has been executed.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

flWorkNetIfParamGwIpAddress

OID	1.3.6.1.4.1.4346.11.11.4.1.4
Syntax	IP address
Access	Read and write
Description	Contains the IP address of the current default gateway/router of the MMS. Modifications only take effect once the "flWorkNetIfParamSave" object has been executed.

The "flWorkNetIfParamAssignment" object must be set to static (1), otherwise objects cannot be written.

flWorkNetIfParamStatus

OID	1.3.6.1.4.1.4346.11.11.4.1.5
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Indicates whether the IP parameters have been modified but not saved:

No change	1
Address setting modified, but not yet activated	2

Address settings must be saved permanently using the "flWorkFWCtrlConfSave" object.

flWorkNetIfParamSave

OID	1.3.6.1.4.1.4346.11.11.4.1.6
Syntax	Integer
Access	Read and write
Description	Provides the option of saving modified IP parameters or undoing the modifications:

Undo modification	1
Activate modification	2

Address settings must be saved permanently using the "flWorkFWCtrlConfSave" object.

flWorkNetIfParamAssignment

OID	1.3.6.1.4.1.4346.11.11.4.1.7
Syntax	Integer
Access	Read and write
Description	Provides the option of modifying the assignment mechanism for IP parameters.

Static IP address 1
Assignment via BootP 2
Assignment via DHCP 3
Assignment via DCP 4

Modifications to the assignment mechanism also affect the management functions via the web interface, via V.24 (RS-232), and Telnet.

Modifications to the assignment mechanism on BootP (2) or DCP (4) are only activated after a restart of the MMS.

Address settings must be saved permanently using the "flWorkFWCtrlConfSave" object.

flWorkNetIfParamManagementVlanId

OID	1.3.6.1.4.1.4346.11.11.4.1.8
Syntax	Integer32 (1 - 4094)
Access	Read and write
Description	If the switch is operated in "Tagging" VLAN mode, this object indicates in which VLAN (VLAN ID) the management agent is located.

flWorkNetPort

OID	1.3.6.1.4.1.4346.11.11.4.2

flWorkNetPortCapacity

OID	1.3.6.1.4.1.4346.11.11.4.2.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Contains the number of available ports depending on the configuration of the MMS.

flWorkNetPortTable

OID	1.3.6.1.4.1.4346.11.11.4.2.2

flWorkNetPortEntry

OID	1.3.6.1.4.1.4346.11.11.4.2.2.1
Description	Generates a table with a detailed description of the port configuration.
flWorkNetPortIndex	

OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Specifies the port number of the selected port.
flWorkNetPortLinkState	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.2
Syntax	Integer
Access	Read
Description	Indicates the port status: Connected 1 Not connected 2 farEndFault 3
flWorkNetPortSpeed	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.3
Syntax	Gauge32
Access	Read
Description	Contains the data transmission rate of the selected port in bps.
flWorkNetPortDuplexMode	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.4
Syntax	Integer
Access	Read
Description	Contains the duplex mode of the selected port: No link 0 Full duplex 1 Half duplex 2
flWorkNetPortNegotiation	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.5
Syntax	Integer
Access	Read
Description	Contains the duplex mode of the selected port: Automatic 1 Manual 2
flWorkNetPortName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.6
Syntax	Octet string (0 - 16)
Access	Read and write
Description	Contains the "name" of the port, e.g., "Robot 1".
flWorkNetPortEnable	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.7
Syntax	Integer
Access	Read and write

OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Specifies the port number of the selected port.
flWorkNetPortLinkState	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.2
Syntax	Integer
Access	Read
Description	Indicates the port status: Connected 1 Not connected 2 farEndFault 3
flWorkNetPortSpeed	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.3
Syntax	Gauge32
Access	Read
Description	Contains the data transmission rate of the selected port in bps.
flWorkNetPortDuplexMode	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.4
Syntax	Integer
Access	Read
Description	Contains the duplex mode of the selected port: No link 0 Full duplex 1 Half duplex 2
flWorkNetPortNegotiation	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.5
Syntax	Integer
Access	Read
Description	Contains the duplex mode of the selected port: Automatic 1 Manual 2
flWorkNetPortName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.6
Syntax	Octet string (0 - 16)
Access	Read and write
Description	Contains the "name" of the port, e.g., "Robot 1".
flWorkNetPortEnable	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.7
Syntax	Integer
Access	Read and write

Description	Here you can disable the port: Port disabled 1 Port enabled 2
flWorkNetPortLinkMonitoring	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.8
Syntax	Integer
Access	Read and write
Description	This object can be used to enable link monitoring (message via display and alarm contact) for the relevant port: Link monitoring enabled 2 Link monitoring disabled 1
flWorkNetPortModus	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.9
Syntax	Integer32 (0 - 1024)
Access	Read and write
escription	This object can be used to set the transmission mode for the relevant port: Auto negotiation 1 10 Mbps half duplex 2 10 Mbps full duplex 3 100 Mbps half duplex 4 100 Mbps full duplex 5 Glass fiber FX ports only support operation at 100 Mbps full duplex (5). The auto crossing function is only active when auto negotiation is enabled. If the transmission speed or transmission mode is set to a fixed value, the auto crossing function is disabled.
flWorkNetPortSTPEnable	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.10
Syntax	Integer
Access	Read and write
Description	This object controls the handling of BPDUs if (Rapid) Spanning Tree is activated: **Firmware with Rapid Spanning Tree Protocol:** RSTP not activated 1 RSTP activated 2 **Firmware with Spanning Tree Protocol:** STP not activated (port is in: Fast forwarding mode 1 STP activated 2
flWorkNetPortIfIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.11
Syntax	Integer32 (0 - 1024)
Access	Read

Description	Contains the index of the port according to IEEE 802.3ad.
flWorkNetLLWHPort	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.12
Syntax	Integer32 (8193 - 8296)
Access	Read
Description	Contains the index of the port according to IEEE 802.3ad, but possibly with gaps (due to missing ports).
flWorkNetPortType	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.13
Syntax	Octet string
Access	Read
Description	Specifies the medium of this port.
flWorkNetPortModuleName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.14
Syntax	Octet string
Access	Read
Description	Specifies the "name" of the module.
flWorkNetPortInterfaceName	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.15
Syntax	Octet string
Access	Read
Description	Specifies the "name" of the interface.
flWorkNetPortPriorityLevel	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.16
Syntax	Integer
Access	Read and write
Description	Selects the priority level for incoming data packets: Priority low 1 (default) Priority high 2
flWorkNetPortPofTransmittingPower	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.17
Syntax	Integer
Access	Read
Description	For polymer fiber (POF) paths < 20 m the transmission power must be reduced. This object can be used to read the switch position on the interface module. Transmission power unknown 1 Reduced transmission power (switch position "OFF") 2 Normal transmission power (switch position "ON") 3
flWorkNetPortStpMode	
OID	1.3.6.1.4.1.4346.11.11.4.2.2.1.18

Syntax	Integer
Access	Read
Description	Specifies the port mode during redundancy operation: Spanning Tree 1 Rapid Spanning Tree 2

flWorkNetPortPoETable

OID 1.3.6.1.4.1.4346.11.11.4.2.3

flWorkNetPortPoEEntry

OID	1.3.6.1.4.1.4346.11.11.4.2.3.1
Description	Generates a table with a detailed description of the PoE port configuration.
flWorkNetPortPoEIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Specifies the port number of the selected port.
flWorkNetPortPoEPowerEnable	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.2
Syntax	Integer
Access	Read and write
Description	Indicates the status of the port in relation to the PoE function: The port can supply power on request 1 The port does **not** supply power on request 2 The PoE status is unknown and cannot be set 3
flWorkNetPortPoECurrentLimitation	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.3
Syntax	Integer
Access	Read and write
Description	This object is used to set the PoE current limitation: Limitation to Class 1 devices or 90 mA 1 No limitation up to the maximum permissible value (350 mA) 2 The PoE status is unknown and cannot be set 3
flWorkNetPortPoEDeviceClass	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.4
Syntax	Integer (0 - 5)
Access	Read

Description	This object contains the detected PoE class of the connected device to the selected port: Class 0 0 Class 1 1 Class 2 2 Class 3 3 Class 4 4 Class 5 5
flWorkNetPortPoEOutputCurrent	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.5
Syntax	Integer (1 - 400)
Access	Read
Description	This object contains the current value of the output current in "mA" of the selected port.
flWorkNetPortPoEOutputVoltage	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.6
Syntax	Integer32 (45000 - 56000)
Access	Read
Description	Indicates the current output voltage at this port in "mV".
flWorkNetPortPoEFaultStatus	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.7
Syntax	Integer
Access	Read
Description	Here you can view the current error status of the port: No error 0 Error in the external PoE supply voltage 1 Temperature too high 2 Current limitation activated 3 Load disconnected 4 The PoE controller does not respond, 48 V supply may be missing 5 No PoE interface module inserted in this slot 6 The switch does not support PoE interface modules 7 No PoE devices connected to this port 8
flWorkNetPortPoEFaultMonitoring	
OID	1.3.6.1.4.1.4346.11.11.4.2.3.1.8
Syntax	Integer
Access	Read and write
Description	This object can be used to enable PoE fault monitoring (message via display and alarm contact) for the relevant port: Fault monitoring enabled 2 Fault monitoring disabled 1

flWorkNetPofScrjIfGroup

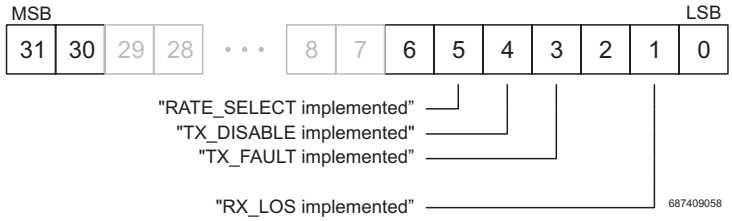
OID 1.3.6.1.4.1.4346.11.11.4.2.4

flWorkNetPortPofScrjIfTable

OID	1.3.6.1.4.1.4346.11.11.4.2.4
Description	Generates a table with a detailed description of the POF-SCRJ port properties
flWorkNetPortPofScrjIfIndex	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Specifies the port number of the selected port.
flWorkNetPortPofScrjIfStatus	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.2
Syntax	Integer
Access	Read
Description	Indicates the status of the port in relation to the POF-SCRJ function The hardware does not support POF-SCRJ diagnostics 1 No POF-SCRJ interface module at this port 2 The system reserve at this port is greater than 2 dB 3 The system reserve is less than 2 dB, but greater than 0 dB 4 No system reserve available - the received optical power is below the required minimum value 5
flWorkNetPortPofScrjIfSupplyVoltage	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.4
Syntax	Integer32 (0 - 65)
Access	Read
Description	This object provides the current supply voltage of the transceiver at this port in 0.1 V increments (possible range: 0 V to 6.5 V).
flWorkNetPortPofScrjIfTxPower	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.6
Syntax	Integer32 (0 - 6553)
Access	Read
Description	This object provides the current transmission power of the transceiver at this port in 0.1 µW increments (possible range: 0 W to 0.006553 W).
flWorkNetPortPofScrjIfRxPower	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.7
Syntax	Integer32 (0 - 6553)
Access	Read
Description	This object provides the current receiving power of the transceiver at this port in 0.1 µW increments (possible range: 0 W to 0.006553 W).
flWorkNetPortPofScrjIfSystemReserve	

OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.8
Syntax	Integer32 (0 - 255)
Access	Read
Description	Provides the remaining system reserve in 0.1 dB increments.
flWorkNetPortPofScrjIfRxPowerHighAlarm	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.9
Syntax	Integer
Access	Read
Description	This object indicates whether the "RX power high" alarm has been triggered: Alarm not triggered 1 Alarm triggered 2
flWorkNetPortPofScrjIfRxPowerLowAlarm	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.10
Syntax	Integer
Access	Read
Description	This object indicates whether the "RX power low" alarm has been triggered: Alarm not triggered 1 Alarm triggered 2
flWorkNetPortPofScrjIfRxPowerHighWarning	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.11
Syntax	Integer
Access	Read
Description	This object indicates whether the "RX power high" warning message has been triggered: Warning message not triggered 1 Warning message triggered 2
flWorkNetPortPofScrjIfRxPowerLowWarning	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.12
Syntax	Integer
Access	Read
Description	This object indicates whether the "RX power low" warning message has been triggered: Warning message not triggered 1 Warning message triggered 2
flWorkNetPortPofScrjIfManufacturer	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.13
Syntax	Octet string
Access	Read
Description	This object provides the name of the manufacturer of the POF-SCRJ transceiver at this port.
flWorkNetPortPofScrjIfManufactOui	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.14
Syntax	Octet string

Access	Read
Description	This object provides the IEEE manufacturer ID of the manufacturer of the POF-SCRJ transceiver at this port.
flWorkNetPortPofScrjIfRevision	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.16
Syntax	Octet string
Access	Read
Description	This object provides the version of the POF-SCRJ transceiver at this port.
flWorkNetPortPofScrjIfWavelength	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.17
Syntax	Integer32
Access	Read
Description	This object provides the wavelength in nm of the POF-SCRJ transceiver at this port.
flWorkNetPortPofScrjIfTransceiverOptions	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.18
Syntax	Integer32
Access	Read
Description	This object provides the implemented functions of the POF-SCRJ transceiver at this port as a bit pattern.



flWorkNetPortPofScrjIfSerialNumber	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.19
Syntax	Octet string
Access	Read
Description	This object provides the serial number of the POF-SCRJ transceiver at this port.
flWorkNetPortPofScrjIfDatecodeAndLot	
OID	1.3.6.1.4.1.4346.11.11.4.2.4.1.20
Syntax	Octet
Access	Read
Description	This object provides the manufacturing date and the delivery number of the POF-SCRJ transceiver at this port as a byte pattern. Byte 1 and 2: Year Byte 3 and 4: Month Byte 5 and 6: Day Byte 7 and 8: Delivery number

flWorkFirmware

OID	1.3.6.1.4.1.4346.11.11.11

flWorkFWInfo

OID	1.3.6.1.4.1.4346.11.11.11.1

flWorkFWInfoVersion

OID	1.3.6.1.4.1.4346.11.11.11.1.1
Syntax	Octet string (4)
Access	Read
Description	Contains the firmware version as a string. Example for Version "3.97": 0x33, 0x2e, 0x39, 0x37.

flWorkFWInfoState

OID	1.3.6.1.4.1.4346.11.11.11.1.2
Syntax	Octet string (6)
Access	Read
Description	Contains the firmware release as a string. Example for "beta": 0x62, 0x65, 0x64, 0x61.

flWorkFWInfoDate

OID	1.3.6.1.4.1.4346.11.11.11.1.3
Syntax	Octet string (6)
Access	Read
Description	Contains the creation date of the firmware version as a string. Example for "21.05.2001": 0x32, 0x31, 0x30, 0x35, 0x30, 0x31.

flWorkFWInfoTime

OID	1.3.6.1.4.1.4346.11.11.11.1.4
Syntax	Octet string (6)
Access	Read
Description	Contains the creation time of the firmware version as a string. Example for "14:10:20": 0x31, 0x34, 0x31, 0x30, 0x32, 0x30.

flWorkFWInfoCopyright

OID	1.3.6.1.4.1.4346.11.11.11.1.5
Syntax	Display string (6)
Access	Read
Description	Contains the owner of the firmware copyright. Copyright by Phoenix Contact GmbH & Co., 2003.

flWorkFWInfoBootVersion

OID	1.3.6.1.4.1.4346.11.11.11.1.6
Syntax	Octet string (4)
Access	Read
Description	Contains the version of the boot loader as a string. Example for Version "2.65": 0x32, 0x2e, 0x36, 0x35.

flWorkFWInfoBootState

OID	1.3.6.1.4.1.4346.11.11.11.1.7
Syntax	Octet string (6)
Access	Read
Description	Contains the boot loader release as a string. Example for "beta": 0x62, 0x65, 0x64, 0x61.

flWorkFWInfoBootDate

OID	1.3.6.1.4.1.4346.11.11.11.1.8
Syntax	Octet string (6)
Access	Read
Description	Contains the creation date of the boot loader version as a string. Example for "09.03.01": 0x30, 0x39, 0x30, 0x33, 0x30, 0x31.

flWorkFWInfoBootTime

OID	1.3.6.1.4.1.4346.11.11.11.1.9
Syntax	Octet string (6)
Access	Read
Description	Contains the creation time of the boot loader version as a string. Example for "14:10:20": 0x31, 0x34, 0x31, 0x30, 0x32, 0x30.

flWorkFWInfoOperStatus

OID	1.3.6.1.4.1.4346.11.11.11.1.11
Syntax	Integer
Access	Read
Description	Contains the operating state of the firmware: - Problem 3 - No error 2 - Other 1

flWorkFWInfoHealthText

OID	1.3.6.1.4.1.4346.11.11.11.1.12

Syntax	Display string
Access	Read
Description	Contains additional information/error states for the firmware.

flWorkFWInfoDisplay

OID	1.3.6.1.4.1.4346.11.11.11.1.13
Syntax	Display string
Access	Read
Description	Contains the current data from the diagnostic display.

flWorkFWCtrl

OID	1.3.6.1.4.1.4346.11.11.11.2

flWorkFWCtrlBasic

OID	1.3.6.1.4.1.4346.11.11.11.2.1

flWorkFWCtrlReset

OID	1.3.6.1.4.1.4346.11.11.11.2.1.1
Syntax	Integer
Access	Read and write
Description	With write access, a reset can be executed with "2". With read access, the value is always "1". When a reset is triggered, "rb" is indicated in the display.

flWorkFWCtrlHttp

OID	1.3.6.1.4.1.4346.11.11.11.2.1.6
Syntax	Integer
Access	Read and write
Description	This object can be used to disable the web server for the switch. The modification only takes effect after a restart:

Web server enabled	2
Web server disabled	1

flWorkFWCtrlTelnet

OID	1.3.6.1.4.1.4346.11.11.11.2.1.7
Syntax	Integer
Access	Read and write
Description	This object can be used to disable the Telnet function for the MMS. The modification only takes effect after a restart:

Telnet activated	2
Telnet deactivated	1

flWorkFWCtrlWebPageRefresh

OID	1.3.6.1.4.1.4346.11.11.11.2.1.8
Syntax	Integer (0 - 3600)
Access	Read and write
Description	Here you can set the refresh time for the automatic update of the web pages in seconds: Default 30 s No update 0 s

flWorkFWCtrlSNMP

OID	1.3.6.1.4.1.4346.11.11.11.2.1.9
Syntax	Integer
Access	Read and write
Description	Here you can activate/deactivate the SNMP agent. The modifications take effect following a restart. SNMP agent deactivated 1 SNMP agent activated 2

flWorkFWCtrlOperatingMode

OID	1.3.6.1.4.1.4346.11.11.11.2.1.10
Syntax	Integer
Access	Read and write
Description	Pre-configuration can be implemented here for "PROFINET" mode. Standard mode (default) 1 PROFINET mode 2

flWorkFWCtrlIfCounters

OID	1.3.6.1.4.1.4346.11.11.11.2.1.11
Syntax	Integer
Access	Read and write
Description	You can reset the statistic values here for all counters from all ports. Not deleted 1 Delete counter 2

flWorkFWCtrlTrapDest

1.3.6.1.4.1.4346.11.11.11.2.2

flWorkFWCtrlTrapDestTable

1.3.6.1.4.1.4346.11.11.11.2.2.1

flWorkFWCtrlTrapDestEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1
Syntax	

Access	
Description	Generates a table with the IP addresses of the trap managers.
flWorkFWCtrlTrapDestIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	Contains the index of the target component, which should receive the traps.
flWorkFWCtrlTrapDestIPAddr	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.1.1.2
Syntax	IP address
Access	Read and write
Description	Contains the IP address of the target component, which should receive the traps.

flWorkFWCtrlTrapDestCapacityMax

OID	1.3.6.1.4.1.4346.11.11.11.2.2.2
Syntax	Integer32
Access	Read
Description	Contains the maximum permissible number of trap receivers.

flWorkFWCtrlTrapDestEnable

OID	1.3.6.1.4.1.4346.11.11.11.2.2.3
Syntax	Integer
Access	Read and write
Description	This object can be used to disable the "send SNMP traps" function: Sending permitted 2 Sending not permitted 1

flWorkFWCtrlTrapLink

OID	1.3.6.1.4.1.4346.11.11.11.2.2.4
Syntax	Integer
Access	Read and write
Description	Here you can specify that the "LinkUp/Down" trap is extended to include a physical port number: Without extension 2 With extension 1

flWorkFWCtrlTrapConnectionTest

OID	1.3.6.1.4.1.4346.11.11.11.2.2.5

Syntax	Integer
Access	Read and write
Description	Here test traps can be sent for a connection test by the SNMP agents.
	Sending test traps 2 No test traps 1

flWorkFWCtrlTrapEnableTable

1.3.6.1.4.1.4346.11.11.11.2.2.10

flWorkFWCtrlTrapEnableEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1
Syntax	
Access	
Description	Generates a table with information about the traps.
flWorkFWCtrlTrapEnableIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1.1
Syntax	Integer32
Access	Read
Description	This object identifies the trap using the trap ID.
flWorkFWCtrlTrapEnableOid	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1.2
Syntax	Object identifier
Access	Read
Description	Indicates the trap OID.
flWorkFWCtrlTrapEnableName	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1.3
Syntax	Display string
Access	Read
Description	This object identifies the trap using the trap name.
flWorkFWCtrlTrapEnableStatus	
OID	1.3.6.1.4.1.4346.11.11.11.2.2.10.1.4
Syntax	Integer
Access	Read/write
Description	This object indicates the transmit status of the trap. While the sending of traps is activated, each trap can be deactivated individually.

flWorkFWCtrlPasswd

OID 1.3.6.1.4.1.4346.11.11.11.2.3

flWorkFWCtrlPasswdSet

OID 1.3.6.1.4.1.4346.11.11.11.2.3.1

Syntax Octet string (2 - 24)

Access Read and write

For security reasons the response is always "******" with read access.

Description A new password can be entered here with a maximum of 12 characters. Example:
- Your new password should be "*factory3*".
- The password must be entered a second time for confirmation.
- Your entry "*factory3factory3*".
- Your password for write access is now: "*factory3*".

flWorkFWCtrlPasswdSuccess

OID 1.3.6.1.4.1.4346.11.11.11.2.3.2

Syntax Integer

Access Read

Description A message is displayed, which informs you whether the last change of password was successful:
- Not changed 1
- Failed 2
- Successful 3

Messages 2 and 3 are displayed for approximately ten minutes after the last access, after which status 1 (not changed) is displayed again.

flWorkFWCtrlLoginExpire

OID 1.3.6.1.4.1.4346.11.11.11.2.3.3

Syntax Integer32 (30 - 3600)

Access Read and write

Description Here, the number of seconds between two password entries is specified as a period of time. After the time has elapsed, the password must be re-entered, if required.

Default 300
Range 30 - 3600

flWorkFWCtrlUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4

flWorkFWCtrlTftpIpAddr

OID	1.3.6.1.4.1.4346.11.11.11.2.4.2
Syntax	IP address
Access	Read and write
Description	This object can be used to set the IP address of the TFTP server for the firmware update.

flWorkFWCtrlTftpFile

OID	1.3.6.1.4.1.4346.11.11.11.2.4.3
Syntax	Octet string (0 - 64)
Access	Read and write
Description	This object can be used to set the name of the firmware file for TFTP download.

flWorkFWCtrlUpdateStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.4.4
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the firmware update:

Update successful	1
Update not successful	2
No update completed	3
Unknown	4

flWorkFWCtrlUpdateExecute

OID	1.3.6.1.4.1.4346.11.11.11.2.4.5
Syntax	Integer
Access	Read and write
Description	This object can be used to trigger the firmware update.

No firmware update	1
Execute firmware update	2

After a firmware update, a reset is required to activate the new firmware.

flWorkFWCtrlRunningUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4.6
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the firmware update:

Firmware update not started	1
Executing firmware update	2
Firmware update successful	3
Connection error	4
Incorrect file name	5
Error	6

flWorkFWCtrlAutoUpdate

OID	1.3.6.1.4.1.4346.11.11.11.2.4.7
Syntax	Integer
Access	Read and write
Description	This object can be used to trigger the firmware update with subsequent restart:

No firmware update	1
Execute firmware update	2

flWorkFWCtrlConf

OID	1.3.6.1.4.1.4346.11.11.11.2.5

flWorkFWCtrlConfStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.1
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the active device configuration:

Configuration OK - configuration corresponds to the saved configuration	1
Configuration faulty - configuration does not correspond to the saved configuration, i.e., after a restart the switch could start with another configuration	2
Configuration saved	3
Saving configuration	4

flWorkFWCtrlConfSave

OID	1.3.6.1.4.1.4346.11.11.11.2.5.2
Syntax	Integer
Access	Read and write
Description	This object can be used to save the device configuration:

Do not save configuration	1
Save configuration	2

flWorkFWCtrlDefaultUponDelivery

OID	1.3.6.1.4.1.4346.11.11.11.2.5.3
Syntax	Integer
Access	Read and write
Description	This object can be used to reset the device to the default settings (see "Default Upon Delivery/Default Settings" on page 3-1). It also triggers a restart: Do not reset to default settings 1 Reset to default settings 2

flWorkFWCtrlConfName

OID	1.3.6.1.4.1.4346.11.11.11.2.5.4
Syntax	Octet string (0 - 64)
Access	Read and write
Description	Here, a descriptive name for the saved configuration can be specified or read.

flWorkFWCtrlConfSource

OID	1.3.6.1.4.1.4346.11.11.11.2.5.5
Syntax	Integer
Access	Read
Description	Here, the storage location of the loaded configuration can be read. Configuration loaded from the device 1 Plug-in parameterization memory 2

flWorkFWConfig

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10

flWorkFWConfigTftpIPAddr

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.2
Syntax	IP address
Access	Read and write
Description	This object can be used to set the IP address of the TFTP server.

flWorkFWConfigTftpFile

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.3
Syntax	Octet string (0 - 64)
Access	Read and write
Description	This object can be used to set the file name for TFTP transmission.

flWorkFWConfigStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.4
Syntax	Integer
Access	Read
Description	This object provides information about the last TFTP transmission called:

Transmission OK	1
Transmission not OK	2
No transmission	3
Unknown	4

flWorkFWConfigExecute

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.5
Syntax	Integer
Access	Read and write
Description	This object can be used to load or save configuration data:

No transmission	1
Transmission from server to switch	2
Transmission from switch to server	3

If the new configuration is not activated by a reset after a configuration download, when the configuration is saved the previously loaded configuration is rejected and instead the active configuration of the MMS is saved.

flWorkFWRunningConfig

OID	1.3.6.1.4.1.4346.11.11.11.2.5.10.6
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the configuration data transmission:

Not started	1
Transmission in progress	2
Transmission successful	3
Connection error	4
Incorrect file/path name	5
Error	6

flWorkFWCtrlConfigMemoryModule (1.3.6.1.4.1.4346.11.11.11.2.5.11)

flWorkFWCtrlConfMemoryModuleStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.1
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the MMS memory module:

Memory module present	1
Memory module working to full capacity	2
Memory module not supported	3
Memory module not present	4
Faulty memory module	5

flWorkFWCtrlConfMemoryModuleClear

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.2
Syntax	Integer
Access	Read and write
Description	Here the memory module can be deleted:

Not deleted	1
Delete memory module	2

flWorkFWCtrlConfMemoryModuleCompare

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.3
Syntax	Integer
Access	Read and write
Description	Here, the configuration comparison between the MMS and memory module can be triggered.

No comparison	1
Compare configuration	2

flWorkFWCtrlConfMemoryModuleCompareStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.4
Syntax	Integer
Access	Read
Description	Here, the configuration comparison between the MMS and memory module can be requested.

Unknown	1
Comparison still running	2
Configuration is the same	3
Configuration is not the same	4
Memory module empty	5

flWorkFWCtrlConfigMemInfo (1.3.6.1.4.1.4346.11.11.11.2.5.11.5)

flWorkFWCtrlConfigMemConfName

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.5.1
Syntax	Octet string
Access	Read
Description	Here the configuration name of the configuration saved in the memory module can be requested.

flWorkFWCtrlConfigMemFwVersion

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.5.2
Syntax	Octet string
Access	Read
Description	Here the firmware version with which the configuration had been saved can be read.

flWorkFWCtrlConfigMemIpAddress

OID	1.3.6.1.4.1.4346.11.11.11.2.5.11.5.3
Syntax	Octet string
Access	Read
Description	Here the IP address of the device that saved this configuration can be read.

flWorkFWCtrlSerial

OID	1.3.6.1.4.1.4346.11.11.11.2.6

flWorkFWCtrlSerialBaud

OID	1.3.6.1.4.1.4346.11.11.11.2.6.1
Syntax	Integer
Access	Read
Description	This object can be used to request the set data transmission rate of the serial interface: 2400 baud 1 9600 baud 2 19200 baud 3 38400 baud 4

flWorkFWCtrlSerialDataBits

OID	1.3.6.1.4.1.4346.11.11.11.2.6.2
Syntax	Integer
Access	Read
Description	Contains the number of data bits in the serial interface: 8 bit 1

flWorkFWCtrlSerialStopBits

OID	1.3.6.1.4.1.4346.11.11.11.2.6.3
Syntax	Integer
Access	Read
Description	Contains the number of stop bits in the serial interface: 1 bit 1 2 bits 2

flWorkFWCtrlSerialParity

OID	1.3.6.1.4.1.4346.11.11.11.2.6.4
Syntax	Integer
Access	Read
Description	Contains the parity mode for the serial interface: None 1 Odd 2 Even 3

flWorkFWCtrlSerialFlowControl

OID	1.3.6.1.4.1.4346.11.11.11.2.6.5
Syntax	Integer
Access	Read
Description	Contains the selected flow control for the serial interface: None 1 Hardware 2

flWorkFWCtrlAlarmContact

OID 1.3.6.1.4.1.4346.11.11.11.2.7

flWorkFWCtrlAlarmContactEvents

OID 1.3.6.1.4.1.4346.11.11.11.2.7.1

flWorkFWCtrlAlarmContactEventPowerSupply

OID	1.3.6.1.4.1.4346.11.11.11.2.7.1.1
Syntax	Integer
Access	Read and write
Description	This object can be used to set the indication of redundant power supply failure via the alarm contact: Monitoring disabled 1 Monitoring enabled 2

flWorkFWCtrlAlarmContactEventLinkState

OID	1.3.6.1.4.1.4346.11.11.11.2.7.1.2
Syntax	Integer
Access	Read and write
Description	This object can be used to set the link down indication for the ports via the alarm contact: Monitoring disabled 1 Monitoring enabled 2

The "flWorkNetPortLinkMonitoring" object can be used to set port monitoring individually for each port.

flWorkFWCtrlAlarmContactEventSecurityPortBlocked

OID	1.3.6.1.4.1.4346.11.11.11.2.7.1.3
Syntax	Integer
Access	Read and write
Description	Indication via the alarm contact if a disabled MAC address accesses a port. Not activated 1 Activated 2

flWorkFWCtrlAlarmContactEventPoEFaultDetected

OID	1.3.6.1.4.1.4346.11.11.11.2.7.1.4
Syntax	Integer
Access	Read and write
Description	Indication via the alarm contact if a PoE fault has occurred. Indication via the alarm contact not activated 1 Indication via the alarm contact activated 2

flWorkFWCtrlAlarmContactEnable

OID	1.3.6.1.4.1.4346.11.11.11.2.7.2
Syntax	Integer
Access	Read and write
Description	This object can be used to set the indication for the configured states via the alarm contact: Monitoring disabled 1 Monitoring enabled 2

flWorkFWCtrlAlarmContactStatus

OID	1.3.6.1.4.1.4346.11.11.11.2.7.3
Syntax	Integer
Access	Read
Description	This object can be used to request the status of the alarm contact: Alarm contact open 1 Alarm contact closed 2

flWorkFWCtrlAlarmContactReason

OID	1.3.6.1.4.1.4346.11.11.11.2.7.4
Syntax	Display string
Access	Read
Description	Indicates the reason why the alarm contact was opened.

flWorkFWCtrlSecurity

OID 1.3.6.1.4.1.4346.11.11.11.2.8

flWorkFWCtrlSecurityAccess

1.3.6.1.4.1.4346.11.11.11.2.8.1

flWorkFWCtrlSecurityAccessTable

flWorkFWCtrlSecurityAccessEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.1
flWorkFWCtrlSecurityAccessIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.1.1
Syntax	Integer32
Access	Read
Description	Shows the index of the entry in the access table.
flWorkFWCtrlSecurityAccessAddr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.1.2
Syntax	IP address
Access	Read and write
Description	Indicates the IP address of the devices that have access rights for this switch.
flWorkFWCtrlSecurityAccessDescr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.3
Syntax	Octet string (0 - 32)
Access	Read and write
Description	Displays the description of the client that has access rights.
flWorkFWCtrlSecurityAccessRight	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.1.4
Syntax	Integer

Access	Read and write
Description	Displays the access rights of the relevant client: Read-only access 1 Read/write access 2
flWorkFWCtrlSecurityAccessTableCapacityMax	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.1.2
Syntax	Integer32
Access	Read
Description	Specifies the maximum possible number of entries for access to WBM.
flWorkFWCtrlSecurityAccessEnable	
OID	1.3.6.1.4.1.4346.11.11.11.3.1.1.3
Syntax	Integer
Access	Read and write
Description	Here you can specify whether access to WBM is regulated via access rights for individual clients or not (if no valid IP address is specified, "without regulation" is set automatically): Without regulation 1 With regulation 2

flWorkFWCtrlSecurityPort

OID 1.3.6.1.4.1.4346.11.11.11.2.8.2

flWorkFWCtrlSecurityPortTable

flWorkFWCtrlSecurityPortEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1
flWorkFWCtrlSecurityPortIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.1
Syntax	Integer32
Access	Read
Description	Displays the index of the entry in the port list.
flWorkFWCtrlSecurityPortLastMacAddr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.2
Syntax	MAC address
Access	Read
Description	Displays the last MAC address that sent frames to this port.
flWorkFWCtrlSecurityPortMode	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.3
Syntax	Integer
Access	Read and write

Description	Displays the security mode of the port or modifies it: No security mode activated 1 For unauthorized access only trap transmission 2 In the event of unauthorized access the port is blocked 3 In the event of unauthorized access the port is blocked with automatic enabling later on 4
flWorkFWCtrlSecurityPortState	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.4
Syntax	Integer
Access	Read and write
Description	Displays the security state of the port or modifies it: Port reenabled (OK) 1 Port is currently blocked 2 Port is currently blocked, will be enabled automatically later on 3 If the port continues to receive packets from illegal MAC addresses, the port will immediately switch to one of the blocked modes.
flWorkFWCtrlSecurityPortIllegalAddrCounter	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.1.1.5
Syntax	Gauge32
Access	Read
Description	Specifies the number of unauthorized MAC addresses that have been registered at this port.

flWorkFWCtrlSecurityPortMacTable

flWorkFWCtrlSecurityPortMacEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.2.1
flWorkFWCtrlSecurityPortMacIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.2.1.1
Syntax	Integer32
Access	Read
Description	Displays the port number.
flWorkFWCtrlSecurityPortMacAddr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.2.1.2
Syntax	MAC address
Access	Read and write
Description	Displays the authorized MAC addresses for this port.
flWorkFWCtrlSecurityPortMacDescr	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.2.1.3

Syntax	Octet string (0 - 16)
Access	Read and write
Description	Displays the user description of the MAC address.

flWorkFWCtrlSecurityPort

flWorkFWCtrlSecurityPortTableCapacityMax	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.3
Syntax	Integer32
Access	Read
Description	Specifies the maximum possible number of entries in the security port table.
flWorkFWCtrlSecurityPortMacTableCapacityMax	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.4
Syntax	Integer32
Access	Read
Description	Displays the maximum number of authorized MAC addresses per port.
flWorkFWCtrlSecurityPortEnable	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.5
Syntax	Integer
Access	Read and write
Description	Indicates whether the safety mechanism for this port is active. If no valid MAC address has been defined, the mechanism is deactivated. Mechanism deactivated 1 Mechanism activated 2
flWorkFWCtrlSecurityPortIllegalAddrCounterClear	
OID	1.3.6.1.4.1.4346.11.11.11.2.8.2.6
Syntax	Integer
Access	Read and write
Description	Deletes all counters for unauthorized addresses. During read access (1 - not deleted) is always transmitted. Not deleted 1 Delete 2

flWorkFWCtrlProfinet

flWorkFWCtrlProfinetAlarm

flWorkFWCtrlProfinetAlarmPortTable

flWorkFWCtrlProfinetAlarmPortEntry	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1
flWorkFWCtrlProfinetAlarmPortIndex	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.1
Syntax	Integer32 (1 - 1024)
Access	Read

Description	Displays the port number.
flWorkFWCtrlProfinetAlarmPortLinkMonitoring	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.2
Syntax	Integer
Access	Read and write
Description	In PROFINET mode, a slot can send an alarm if the link status changes from "Connected" to "Not connected": Do not send alarm 1 Send alarm 2
flWorkFWCtrlProfinetAlarmPortPofScrjDiag	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.3
Syntax	Integer
Access	Read and write
Description	In PROFINET mode, a slot can send an alarm if the transmission power of a POF-SCRJ port reaches a critical value or the port enters a critical state: Do not send alarm 1 Send alarm 2
flWorkFWCtrlProfinetAlarmPowerSupply	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.10
Syntax	Integer
Access	Read and write
Description	In PROFINET mode, the switch can send an alarm if one of the redundant power supplies fails: Do not send alarm 1 Send alarm 2
flWorkFWCtrlProfinetAlarmModuleRemove	
OID	1.3.6.1.4.1.4346.11.11.11.2.9.1.1.1.11
Syntax	Integer
Access	Read and write
Description	In PROFINET mode, the switch can send an alarm if one of the interface modules is removed: Do not send alarm 1 Send alarm 2

flSwitch

OID 1.3.6.1.4.1.4346.11.11.15

flSwitchCtrl

OID 1.3.6.1.4.1.4346.11.11.15.1

flSwitchCtrlSpanTree

OID	1.3.6.1.4.1.4346.11.11.15.1.1
Syntax	Integer
Access	Read and write
Description	Activates/deactivates STP for the switch.

STP deactivated	1
STP activated	2

To enable STP activation, the "flSwitchCtrlRedundancy" object must be set to STP.

flSwitchCtrlRedundancy

OID	1.3.6.1.4.1.4346.11.11.15.1.2
Syntax	Integer
Access	Read and write
Description	Displays the selected redundancy mechanisms for the switch. If "No redundancy" is selected, all redundancy mechanisms and the corresponding web pages are disabled. If RSTP is activated, the web pages for RSTP are enabled.

No redundancy	1
RSTP activated	2

For STP configuration, the Bridge_MIB is used, see page 4-59.

flSwitchCtrlMulticast

OID	1.3.6.1.4.1.4346.11.11.15.1.3
Syntax	Integer
Access	Read and write
Description	Indicates whether the web pages required for multicast operation are displayed.

Hide web pages	1
Show web pages	2

flSwitchCtrlVLAN

OID	1.3.6.1.4.1.4346.11.11.15.1.4
Syntax	Integer
Access	Read and write
Description	Indicates whether the web pages required for VLAN configuration are enabled.
	VLAN web pages hidden 1 VLAN web pages shown 2

flSwitchCtrlVLANTagMode

OID	1.3.6.1.4.1.4346.11.11.15.1.5
Syntax	Integer
Access	Read and write
Description	In "Transparent" mode the switch ignores the VLAN ID and forwards packets according to their priority alone. In "Tagging" mode, the packets are forwarded according to the regulation.
	Transparent 1 Tagging 2

flSwitchCtrlVLANTagStatus

OID	1.3.6.1.4.1.4346.11.11.15.1.6
Syntax	Integer
Access	Read
Description	Displays the current VLAN mode of the switch.
	Transparent 1 Tagging 2

flSwitchCtrlLldp

OID	1.3.6.1.4.1.4346.11.11.15.1.7
Syntax	Integer
Access	Read and write
Description	This object can be used to enable/disable the LLDP (Link Layer Discovery Protocol):
	LLDP deactivated 1 LLDP activated 2 Send 3 Receive 4

flSwitchCtrlRSTPLargeTreeSupport

OID	1.3.6.1.4.1.4346.11.11.15.1.8
Syntax	Integer
Access	Read and write
Description	When in RSTP large tree mode, the number of switches that can be connected to the root can be increased from 7 to 28 switches: Up to 7 switches in the root 1 Up to 28 switches in the root 2

flSwitchCtrlHashMode

OID	1.3.6.1.4.1.4346.11.11.15.1.9
Syntax	Integer
Access	Read and write
Description	This object can be used to set the search method for the switch in the MAC address table: Optimized search method for randomly saved MAC addresses (default) 1 Optimized search method for MAC addresses saved in ascending order 2

flSwitchCtrlDhcpRelayAgentUi

OID	1.3.6.1.4.1.4346.11.11.15.1.10
Syntax	Integer
Access	Read and write
Description	This object can be used to hide or show the configuration page for the DHCP relay agent in WBM: Hide DHCP relay agent configuration page 1 Show DHCP relay agent configuration page (default) 2

flSwitchCtrlMacTableErase

OID	1.3.6.1.4.1.4346.11.11.15.1.11
Syntax	Integer
Access	Read and write
Description	This object can be used to enable the switch to delete all entries from its MAC address table: Do not delete MAC address table 1 Delete MAC address table 2

flSwitchPortMirr

OID	1.3.6.1.4.1.4346.11.11.11.15.2

flSwitchPortMirrDestinationPort

OID	1.3.6.1.4.1.4346.11.11.11.15.2.1
Syntax	Integer32
Access	Read and write
Description	This object can be used to set the port (destination port), which mirrors the data of another port (source port): No port mirroring 0

flSwitchPortMirrSourcePort

OID	1.3.6.1.4.1.4346.11.11.11.15.2.2
Syntax	Integer32
Access	Read and write
Description	This object can be used to set the port (source port), whose data is to be mirrored to another port (destination port): No port mirroring 0

flSwitchPortMirrStatus

OID	1.3.6.1.4.1.4346.11.11.11.15.2.3
Syntax	Integer
Access	Read and write
Description	This object can be used to enable/disable port mirroring: No port mirroring: 1 Port mirroring enabled 2

Port mirroring is disabled if one (or both) of the "**flSwitchPortMirrDestinationPort"** and "**flSwitchPortMirrSourcePort**" objects contains the value "0" or if they contain the same value (e.g., both set to 2).

flSwitchIgmp

OID 1.3.6.1.4.1.4346.11.11.15.3

flSwitchIgmpSnoop

OID 1.3.6.1.4.1.4346.11.11.15.3.1

flSwitchIgmpSnoopEnable

OID	1.3.6.1.4.1.4346.11.11.15.3.1.1
Syntax	Integer
Access	Read and write
Description	Here, the IGMP snooping function can be activated: Deactivated 1 Activated 2

flSwitchIgmpSnoopAging

OID	1.3.6.1.4.1.4346.11.11.15.3.1.3
Syntax	Integer (30 - 3600)
Access	Read and write
Description	Here, the duration of the timeout period for the multicast groups dynamically learned (via IGMP) can be entered in seconds.

flSwitchIgmpSnoopTable

OID	1.3.6.1.4.1.4346.11.11.15.3.1.4

flSwitchIgmpSnoopEntry

OID	1.3.6.1.4.1.4346.11.11.15.3.1.4.1

flSwitchIgmpSnoopEgressPorts

OID	1.3.6.1.4.1.4346.11.11.15.3.1.4.1.1
Syntax	PortList
Access	Read
Description	This object displays the ports that forward multicast data due to IGMP snooping.

flSwitchIgmpSnoopExtended

flSwitchBlockUnknownMulticastAtQuerier

OID	1.3.6.1.4.1.4346.11.11.15.3.1.5.1
Syntax	Integer
Access	Read and write
Description	If this function is activated, the switch only forwards multicast packets if it received membership reports in advance.

Activated	2
Deactivated	1

flSwitchForwardUnknownMulticastToQuerier

OID	1.3.6.1.4.1.4346.11.11.15.3.1.5.2
Syntax	Integer
Access	Read and write
Description	

flSwitchIgmpQuery

OID 1.3.6.1.4.1.4346.11.11.15.3.2

flSwitchIgmpQueryTable

OID 1.3.6.1.4.1.4346.11.11.15.3.2.1

flSwitchIgmpQueryEntry

1.3.6.1.4.1.4346.11.11.15.3.2.1.1

flSwitchIgmpQueryPorts

OID	1.3.6.1.4.1.4346.11.11.15.3.2.1.1.1
Syntax	Port list
Access	Read
Description	This object displays the ports that received the IGMP router query BPDUs.

flSwitchIgmpQueryEnable

OID	1.3.6.1.4.1.4346.11.11.15.3.2.2
Syntax	Integer
Access	Read and write
Description	This object can be used to specify the protocol version that the switch uses to transmit IGMP queries. Deactivated: 1 Version 1: 2 Version 2: 3

flSwitchIgmpQueryInterval

OID	1.3.6.1.4.1.4346.11.11.15.3.2.3
Syntax	Integer
Access	Read and write
Description	This object can be used to specify the time interval during which the switch transmits IGMP queries. Default: 125 s Permissible value range: 10 s to 3600 s (in increments of 1 s)

flSwitchIgmpTableErase

OID	1.3.6.1.4.1.4346.11.11.15.3.3
Syntax	Integer
Access	Read and write
Description	This object can be used to enable the switch to delete all entries from its IGMP table: Do not delete IGMP table 1 Delete IGMP table 2

flSwitchRedundancy

OID	1.3.6.1.4.1.4346.11.11.15.4

flSwitchCtrlRSTPFastRingDetection

OID	1.3.6.1.4.1.4346.11.11.15.4.1
Syntax	Integer
Access	Read and write
Description	This object can be used to specify whether you wish to use standard RSTP or also fast ring detection as well: Standard RSTP 1 Fast ring detection 2

flSwitchRSTPRingTable

OID	1.3.6.1.4.1.4346.11.11.15.4.2
	flSwitchRSTPRingEntry
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1
	flSwitchRSTPRingIndex
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.1
Syntax	Integer (1 - 1024)
Access	Read
Description	This object specifies the RSTP ring number
flSwitchRSTPRingMAC	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.2
Syntax	MAC address
Access	Read
Description	This object specifies the MAC address of the switch, which forms the alternative port/path in this ring.
flSwitchRSTPRingBlockPort	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.3
Syntax	Integer32
Access	Read
Description	This object specifies the number of the blocked port in this ring.
flSwitchRSTPRingRootPort	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.4
Syntax	Integer32
Access	Read
Description	This object specifies the number of the local port (often the root port) in this ring.
flSwitchRSTPRingDesPort	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.5

Syntax	Integer32
Access	Read
Description	This object specifies the number of a local port (designated port) in this ring.
flSwitchRSTPRingStatus	
OID	1.3.6.1.4.1.4346.11.11.15.4.2.1.6
Syntax	Integer
Access	Read
Description	This object specifies the status of the RSTP ring: Ring closed 3 Ring not closed 6 Error 7
flSwitchRSTPRingFailedPort	
OID	1.3.6.1.4.1.4346.11.11.15.4.3
Syntax	Integer32
Access	Read
Description	This object specifies the number of the faulty port in the ring.

flSwitchRelayAgentDHCP

OID 1.3.6.1.4.1.4346.11.11.15.5

flSwitchRelayAgentDhcpCtrl

OID	1.3.6.1.4.1.4346.11.11.15.5.1
Syntax	Integer
Access	Read and write
Description	This object can be used to set the status of the DHCP relay agent: DHCP relay agent deactivated 1 DHCP relay agent activated 2

If DHCP is activated for the assignment of IP parameters, the DHCP relay agent is automatically deactivated.

flSwitchRelayAgentDhcpIpAddress

OID	1.3.6.1.4.1.4346.11.11.15.5.2
Syntax	IP address
Access	Read and write
Description	This object can be used to set the IP address of the DHCP server for the DHCP relay agent (default 0).

	flSwitchRelayAgentDhcpStatus
OID	1.3.6.1.4.1.4346.11.11.15.5.3
Syntax	Octet string (1 - 255)
Access	Read
Description	This object indicates the status of the DHCP relay agent. The status is affected by: – The "flSwitchRelayAgentDhcpCtrl" object – The assignment mechanism for the IP parameters
	flSwitchRelayAgentDhcpRIdType
OID	1.3.6.1.4.1.4346.11.11.15.5.4
Syntax	Integer (IP address (1), MAC address (2))
Access	Read and write
Description	This object indicates whether the DHCP relay agent specifies its MAC address or its IP address as the remote ID when completing the fields for DHCP option 82 (default: IP address).
	flSwitchRelayAgentDhcpPortTable
OID	1.3.6.1.4.1.4346.11.11.15.5.5
	flSwitchRelayAgentDhcpPortEntry

OID	1.3.6.1.4.1.4346.11.11.15.5.5.1
Syntax	
Access	
Description	This table provides port-specific information for the DHCP relay agent
flSwitchRelayAgentDhcpPortCtrlIndex	
OID	1.3.6.1.4.1.4346.11.11.15.5.5.1.1
Syntax	Integer32 (1 - 1024)
Access	Read
Description	This object specifies the port number.
flSwitchRelayAgentDhcpPortCtrlOperation	
OID	1.3.6.1.4.1.4346.11.11.15.5.5.1.2
Syntax	Integer32
Access	Read/write
Description	Here, the DHCP relay agent at this port can be activated or deactivated: DHCP relay agent at this port deactivated: 1 DHCP relay agent at this port activated: 2

4.4 Management via Local V.24 (RS-232) Communication Interface

4.4.1 General Function

A local communication connection can be established to an external management station via the V.24 (RS-232) interface in Mini-DIN format. Use the "PRG CAB MINI DIN" programming cable (Order No. 2730611). The communication connection is established using a corresponding emulation between the switch and a PC (e.g., HyperTerminal under Windows) and enables access to the user interface.

The reference potentials of the V.24 (RS-232) interface and the supply voltage are not electrically isolated.

4.4.1.1 Interface Configuration

Make the following settings on your Windows PC.

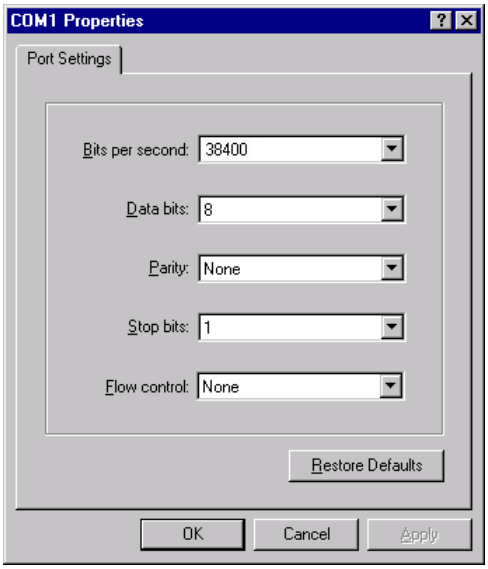


Figure 4-50 Configuring the HyperTerminal

4.4.1.2 Calling the User Interface

Connect the PC and the switch using a suitable cable (PRG CAB MINI DIN, Order No. 2730611). Once you have established the connection, select the Ctrl + L key combination on the PC. The switch then requests the screen contents.

4.4.2 User Interface Functions

4.4.2.1 Functions During the Boot Process After a Restart

If you open the user interface in the first five seconds immediately after an MMS restart, you have the option of triggering a firmware update. Since the actual switch firmware is not yet started at this stage, even in the event of an error, e.g., if the firmware on the device is faulty, this firmware can still be updated (see "Starting With Faulty Software (Firmware)" on page 4-120).

4.4.2.2 Functions During Operation

The following functions are available in the user interface:

– Setting IP parameters
– Selecting the addressing mechanism
– Resetting to the default settings
– Activating/deactivating the web server, the Telnet function, and SNMP
– Activating/deactivating port security, access control for web
– Switching the VLAN mode
– Switching the operating mode
– Activating/deactivating the RSTP redundancy mechanism
– Reset

The activation/deactivation of the web server or Telnet function only takes effect after a "SAVE" and subsequent restart.

All settings are transferred using "APPLY", but are **not** saved permanently. Use the "SAVE" function to save the active configuration settings permanently.

4.4.2.3 Structure of the User Interface Screens

Login Screen

```
Login Screen



          - - - > Phoenix Contact Modular Managed Switch System < - - -
                            Phoenix Contact GmbH & Co. KG
                               www.phoenixcontact.com


                     Running switch application version:   x.xx


                     Password:    [                  ]


                                                                    68740010
```

Figure 4-51 User interface login screen

The login screen indicates the version of the firmware used. A password must be entered to make other settings. By default upon delivery, the password is "private". It is case-sensitive. We strongly recommend that you change the password (via SNMP or WBM).

Basic Switch Configuration

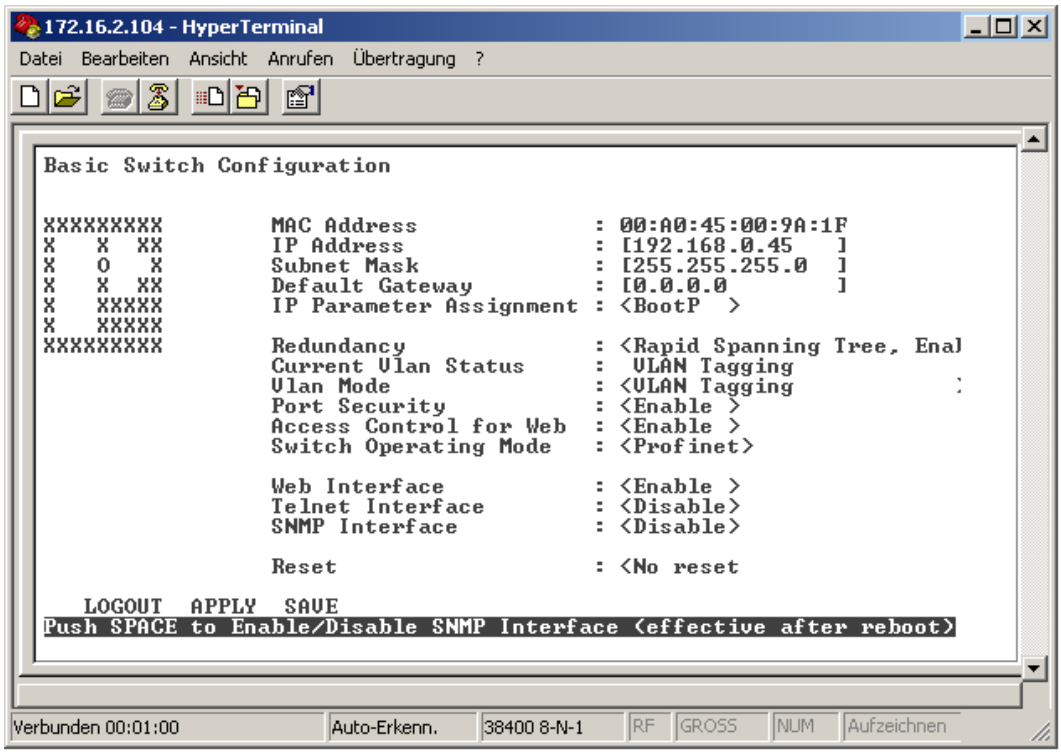


Figure 4-52 IP configuration in the user interface

As well as displaying the set MAC address, this screen can be used to view or modify the IP parameters.

In order to set the IP parameters, the "Static" option must be selected for "IP Parameter Assignment".

This user interface screen can be used to determine the addressing mechanism or to trigger a device restart.

All settings are transferred using "APPLY", but are **not** saved permanently. Use the "SAVE" function to save the active configuration settings permanently.

Resetting to the Default Settings

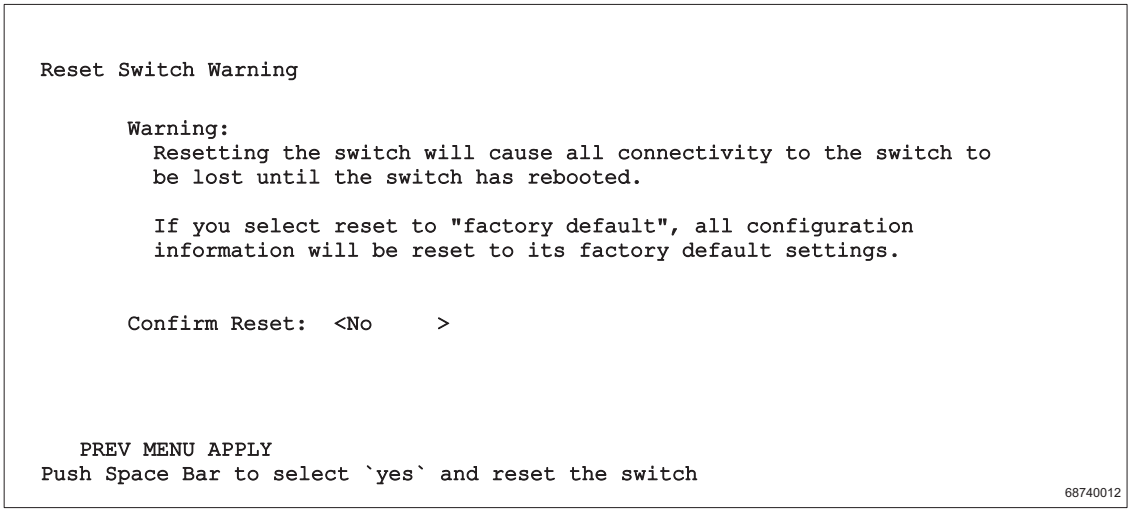

Reset Switch Warning
Warning:
Resetting the switch will cause all connectivity to the switch to be lost until the switch has rebooted.
If you select reset to "factory default", all configuration information will be reset to its factory default settings.
Confirm Reset: <No >
PREV MENU APPLY
Push Space Bar to select `yes` and reset the switch
68740012

Figure 4-53 Resetting to the default settings

This screen can be used to reset the switch to the settings default upon delivery or to restart it. This screen can be opened by first setting the "Reset Switch" option or the "Reset Switch to factory defaults" option in the "Basic Switch Configuration" screen, and then selecting "Apply" or "Save". This undoes any changes to the configuration, and resets all IP parameters to the settings default upon delivery (see Section 3.1.1 on page 3-1).

Resetting to the default settings also resets the password to "private". For security reasons, we recommend you enter a new, unique password.

4.4.3 Starting With Faulty Software (Firmware)

If the software (firmware) installed on the MMS is faulty, you can restore or update the firmware using an update. Observe the 7-segment display (see also page 1-15).

Procedure:

– Connect the switch to your PC via the serial V.24 (RS-232) interface. Make sure that your HyperTerminal is configured correctly (see configuration on page 4-116).
– Restart the switch.

```
- - - > Phoenix Contact Modular Managed Switch System < - - -

Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com
BIOS version: X.XX


Press any key to stop booting ...
1

ENTER ´a´  TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´  TO CONTINUE BOOTING

PxC MMS systemprompt
```

68740010

Figure 4-54 Screen displayed on HyperTerminal when booting

If the device firmware is faulty, the following message appears:

```
   - - - > Phoenix Contact Modular Managed Switch System < - - -
                  Phoenix Contact GmbH & Co. KG
                     www.phoenixcontact.com


Press any key to stop booting ...
 0
booting continues ...

SOFTWARE IMAGE CORRUPTED

YOU HAVE TO UPDATE THE SOFTWARE USING XMODEM PROTOCOL:

ENTER ´a´ TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´ TO CONTINUE BOOTING

PxC MMS systemprompt>
```

68740024

Figure 4-55 Selection menu for faulty firmware

Press "a" to download the new software. The following message appears:

```
   - - - > Phoenix Contact Modular Managed Switch System < - - -
                  Phoenix Contact GmbH & Co. KG
                     www.phoenixcontact.com



ENTER ´a´ TO DOWNLOAD SWITCH SOFTWARE USING XMODEM PROTOCOL
ENTER ´c´ TO CONTINUE BOOTING

PxC MMS systemprompt> a

Downloading firmware image with XMODEM over serial port ...

XMODEM Receive: Waiting for Sender ...

-_
```

68740025

Figure 4-56 XMODEM ready

The switch is now ready for the new firmware. In HyperTerminal, select "Send File" from the "Transmission" menu.

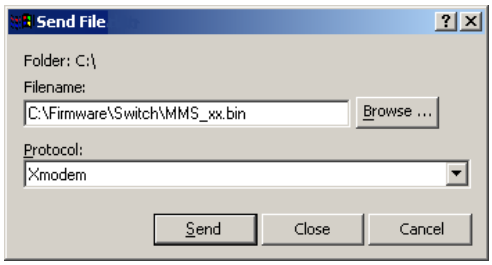


Figure 4-57 Xmodem - Send File option

Make sure that the protocol is set to "Xmodem", otherwise the transmission will fail.

Clicking "Send" starts the file transfer. The following screen shows the progress of the file transmission.

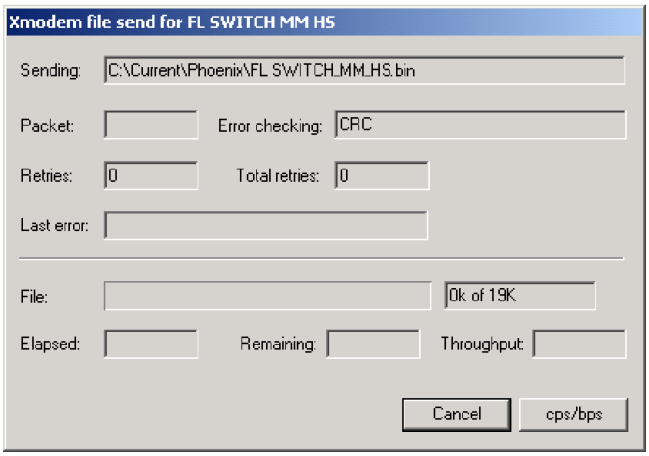


Figure 4-58 File transmission with Xmodem

File transmission may take a few minutes. Do not perform any other actions while the box is open.

Once the box has closed, a message appears in HyperTerminal. Enter "c" to continue with the boot process, or trigger a reset using the reset button.

4.5 Management via Telnet

The Telnet protocol provides the function of a virtual terminal. It offers remote access from a specific computer to other systems in the network (e.g., PCs or MMS). Telnet uses TCP/IP on the network, supports the functions of Layers 5 to 7, and provides bidirectional communication for linking data termination devices with the relevant processes. The destination system is generally referred to as the Telnet server, while the specific local system is the Telnet client. It is only possible to connect a Telnet client and Telnet server. The Telnet server appears to the client as a locally connected terminal.

4.5.1 Configuring the Telnet Terminal

For a Telnet connection to be established between the PC and the MMS, the IP parameters of both devices must be adjusted so that they are in the same subnetwork.

Establishing the Telnet Connection

Connect the PC and the switch to an Ethernet network. From the Start menu, select the "Run..." option. Enter the following command and the IP address of the MMS. Click "OK" to establish the connection with the switch.

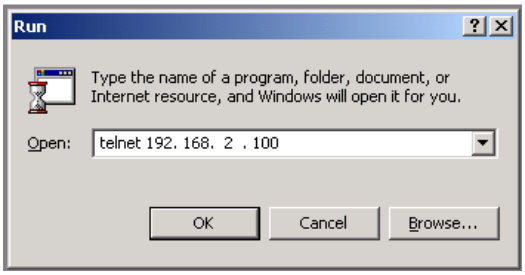

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
telnet 192. 168. 2 . 100
OK
Cancel
Browse...

Figure 4-59 Establishing the Telnet connection

4.5.2 Telnet Interface Functions

The following functions are available in the Telnet interface:

– Setting IP parameters
– Selecting the addressing mechanism
– Resetting to the default settings
– Activating/deactivating the web server, the Telnet function, and SNMP
– Activating/deactivating port security, access control for web
– Switching the VLAN mode
– Switching the operating mode
– Activating/deactivating the RSTP redundancy mechanism
– Reset

All settings are transferred using "APPLY", but are **not** saved permanently. Use the "SAVE" function to save the active configuration settings permanently.

Structure of the Telnet Interface Screens

Login Screen

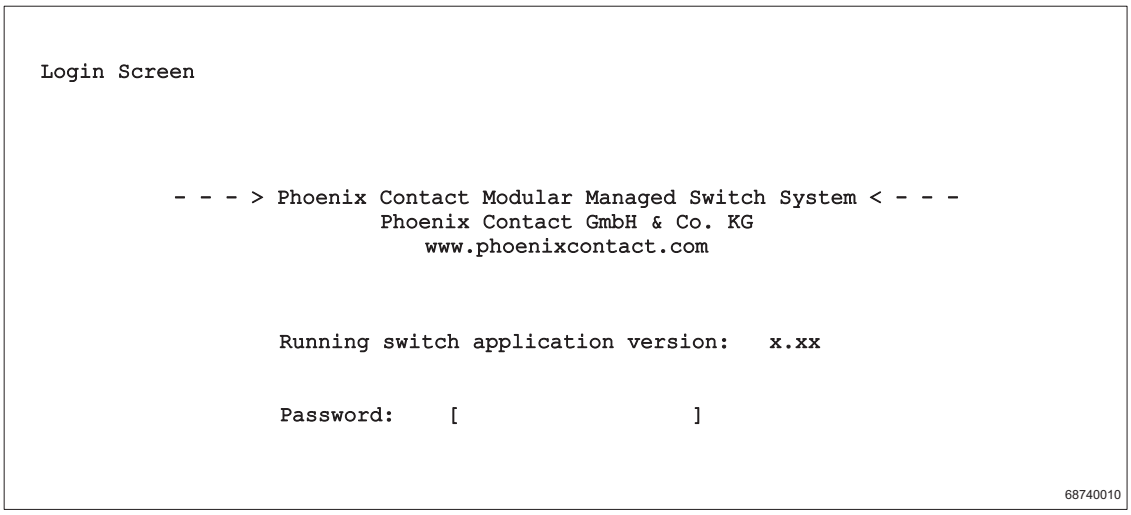

Login Screen
- - - > Phoenix Contact Modular Managed Switch System < - - -
Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com
Running switch application version: x.xx
Password: [ ]
68740010

Figure 4-60 User interface login screen

The login screen indicates the version of the firmware used. A password must be entered to make other settings. By default upon delivery, the password is "private". It is case-sensitive. We strongly recommend that you change the password.

Basic Switch Configuration

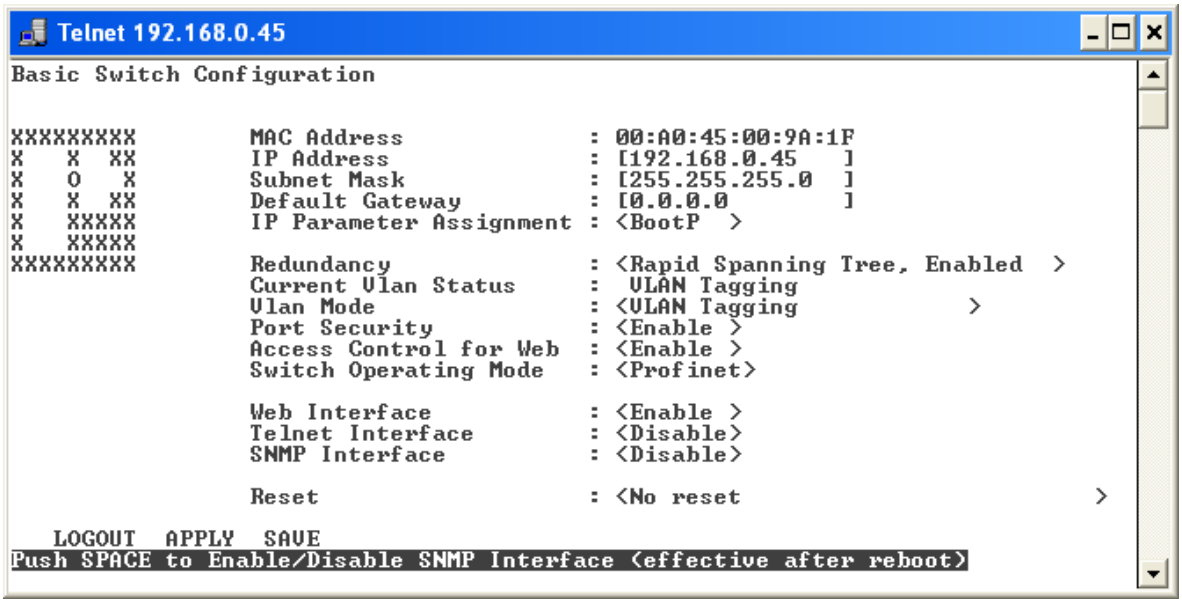


Figure 4-61 IP configuration in the user interface

As well as displaying the set MAC address, this screen can be used to view or modify the IP parameters.

In order to set the IP parameters, the "Static" option must be selected for "IP Parameter Assignment".

All settings are transferred using "APPLY", but are **not** saved permanently. Use the "SAVE" function to save the active configuration settings permanently.

Resetting to the Default Settings

Select "Reset" in the "Basic Switch Configuration" screen. The type of reset can now be selected.

```
Reset Switch Warning

       Warning:
         Resetting the switch will cause all connectivity to the switch to
         be lost until the switch has rebooted.

         If you select reset to "factory default", all configuration
         information will be reset to its factory default settings.


       Confirm Reset:  <No     >



   PREV MENU APPLY
Push Space Bar to select `yes` and reset the switch
```

68740012

Figure 4-62 Resetting to the default settings

This screen can be used to reset the switch to the default settings. This undoes any changes to the configuration, and resets all IP parameters to the settings default upon delivery (see Section 3.1.1 on page 3-1).

Resetting to the default settings also resets the password to "private". For security reasons, we recommend you enter a new, unique password.

5 (Rapid) Spanning Tree

5.1 General Function

Loops

The Rapid/Spanning Tree Protocol (RSTP) is a standardized method (IEEE 802.802.1w/IEEE 802.1d) that enables the use of Ethernet networks with redundant data paths. Ethernet networks with redundant data paths form a meshed topology with impermissible loops. Due to these loops, data packets can circulate endlessly within the network and can also be duplicated. As a consequence, the network is usually overloaded due to circulating data packets and thus communication is interrupted. The meshed structure is thus replaced by a logical, deterministic path with a tree structure without loops using the Spanning Tree algorithm. In the event of data path failure, some of the previously disconnected connections are reconnected to ensure uninterrupted network operation.

IEEE 802.1w

The Rapid Reconfiguration Spanning Tree Protocol (RSTP) is a standardized method (IEEE 802.1w) that enables the use of Ethernet networks with redundant data paths and prevents the long timer-controlled switch-over times of STP. Usually, the formal term "Rapid Reconfiguration Spanning Tree" is not used, rather just "Rapid Spanning Tree Protocol ((R)STP)".

Example:

In the following network topology (six) redundant paths have been created to ensure access to all network devices in the event of a data path failure. These redundant paths are impermissible loops. The Spanning Tree Protocol automatically converts this topology into a tree by disconnecting selected ports. In this context, one of the switches is assigned the role of the root of the tree. From this root, all other switches can be accessed by via a single data path.

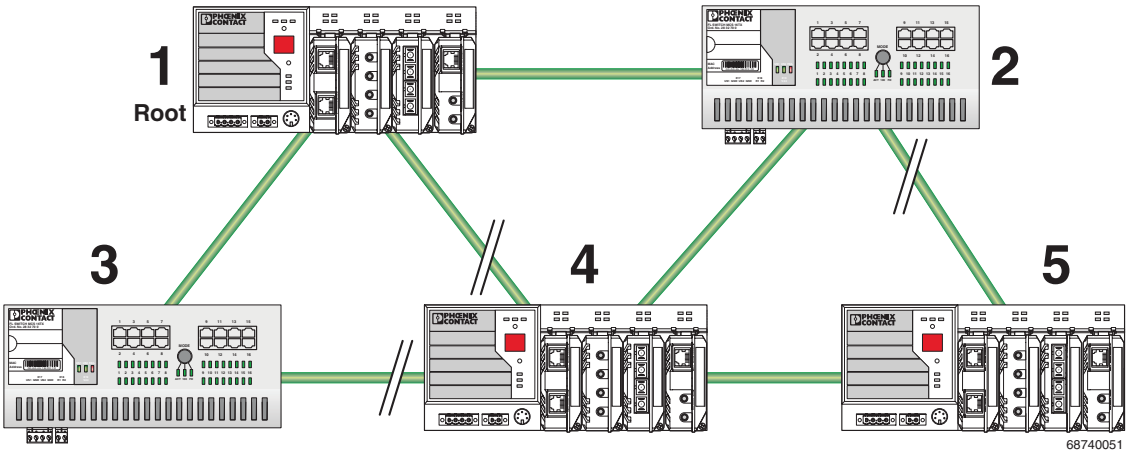


Figure 5-1 Possible tree structure with Spanning Tree

5.2 (R)STP Startup

Startup consists of two parts that must be executed in the specified order:

1 Enable (R)STP on all switches that are to be operated as active (R)STP components in the network.

2 Connect the switches to form a meshed topology.

Only create the meshed topology after activating (R)STP.

5.2.1 Enabling (R)STP on All Switches Involved

(R)STP can be activated via web-based management, via the SNMP interface, via the serial interface or via Telnet.

While learning the network topology, the switch temporarily does not participate in network communication.

5.2.1.1 Enabling With Web-Based Management

Activate web-based management for the switches, e.g., using the Factory Manager. Switch to the "General Configuration" menu, then the "User Interfaces" page. Activate the "(Rapid) Spanning Tree" function under "Redundancy" and confirm by entering your password.

When activating "(Rapid) Spanning Tree" under "User Interfaces", the redundancy mechanism is **not** activated. In the WBM menu, the "(Rapid) Spanning Tree" page - under which the function can be configured and activated - is enabled.

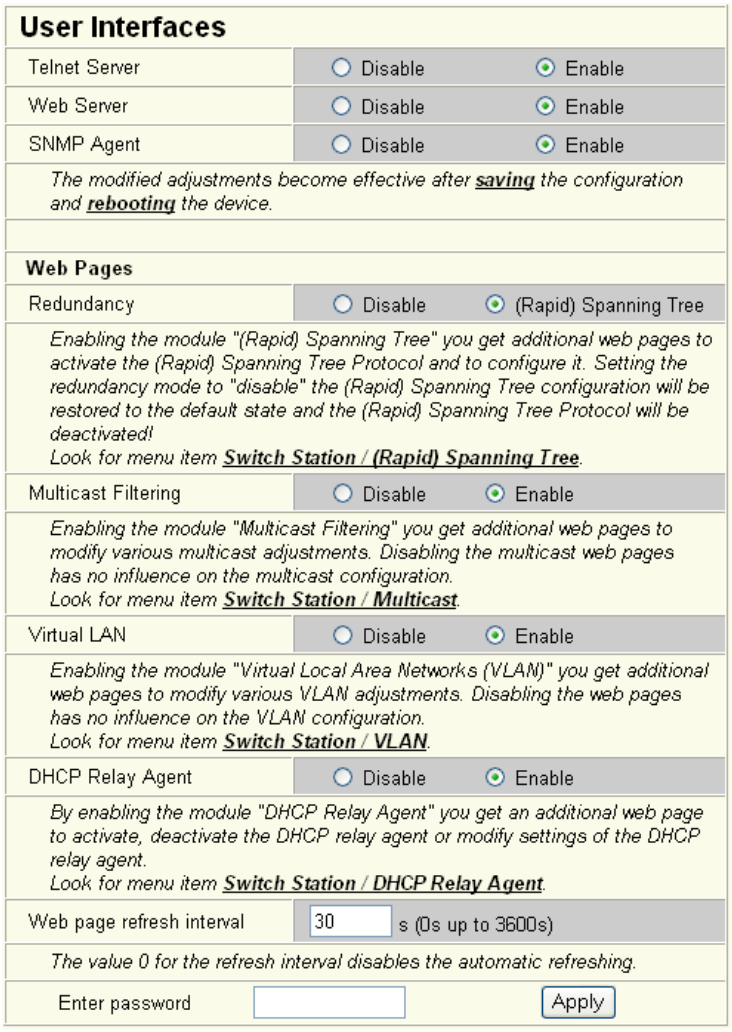

User Interfaces
Telnet Server
Disable
Enable
Web Server
Disable
Enable
SNMP Agent
Disable
Enable
The modified adjustments become effective after saving the configuration and rebooting the device.
Web Pages
Redundancy
Disable
(Rapid) Spanning Tree
Enabling the module "(Rapid) Spanning Tree" you get additional web pages to activate the (Rapid) Spanning Tree Protocol and to configure it. Setting the redundancy mode to "disable" the (Rapid) Spanning Tree configuration will be restored to the default state and the (Rapid) Spanning Tree Protocol will be deactivated!
Look for menu item Switch Station / (Rapid) Spanning Tree.
Multicast Filtering
Disable
Enable
Enabling the module "Multicast Filtering" you get additional web pages to modify various multicast adjustments. Disabling the multicast web pages has no influence on the multicast configuration.
Look for menu item Switch Station / Multicast.
Virtual LAN
Disable
Enable
Enabling the module "Virtual Local Area Networks (VLAN)" you get additional web pages to modify various VLAN adjustments. Disabling the web pages has no influence on the VLAN configuration.
Look for menu item Switch Station / VLAN.
DHCP Relay Agent
Disable
Enable
By enabling the module "DHCP Relay Agent" you get an additional web page to activate, deactivate the DHCP relay agent or modify settings of the DHCP relay agent.
Look for menu item Switch Station / DHCP Relay Agent.
Web page refresh interval
30
s (0s up to 3600s)
The value 0 for the refresh interval disables the automatic refreshing.
Enter password
Apply

Figure 5-2 "User Interfaces" menu

The previously created configuration is lost and the web pages for (R)STP are hidden if "Redundancy" is set to "Disable" on the "User Interfaces" web page following (R)STP configuration.

Now switch to the "(R)STP General" page in the "Switch Station" menu. Here, you will find various information about the Spanning Tree configuration.

(R)STP General	
(Rapid) Spanning Tree Status	This bridge is the **root** bridge!
System Up Time	1 days 18 hours 36 minutes 9 seconds
Last Topology Change	1 days 18 hours 36 minutes 3 seconds ago
Topology Changes	1
Designated Root	8000 00:A0:45:00:9A:1F
Root Port	0
Root Cost	0
Maximum Age of STP Information	20s
Hello Time	2s
Forward Delay	15s
Note: This web page will be refreshed in 1 sec automatically (change the interval at the web page 'Services')!	

Figure 5-3 (R)STP General

The web page displays the parameters with which the switch is currently operating.

(R)STP Configuration

It is sufficient to set the Rapid Spanning Tree status to "Enable" in order to start (R)STP using default settings. Priority values can be specified for the switch. The bridge and backup root can be specified via these priority values.

Only multiples of 4096 are permitted. The desired value can be entered in the "Priority" field. The value will be rounded automatically to the next multiple of 4096. Once you have confirmed the modification by entering your password, the initialization mechanism is started.

Redundant connections can now be created.

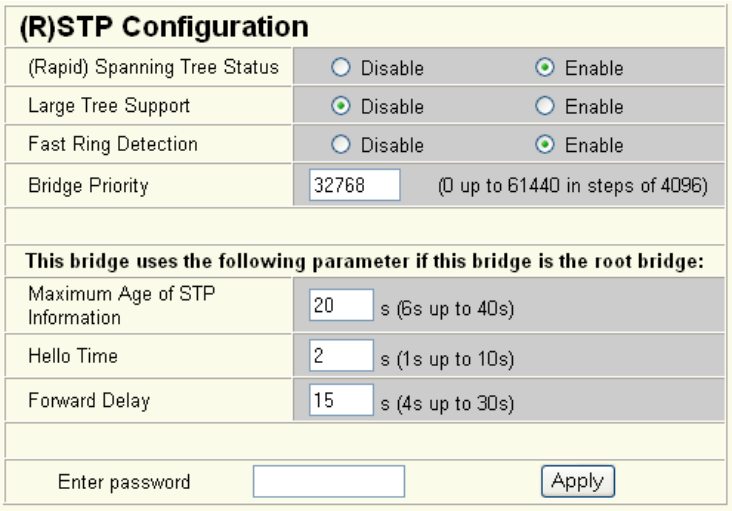


Figure 5-4 (R)STP Configuration

Large Tree Support
If RSTP is operated using the default values, it is suitable for up to seven switches along the relevant path (see Figure 5-18 on page 5-24 and Figure 5-19 on page 5-25 as an example for the relevant path). The RSTP protocol would therefore be possible in a ring topology for up to 15 switches.

The "Large Tree Support" option makes the ring topology suitable for 28 switches along the relevant path if RSTP is used. The large tree support option could provide an RSTP ring topology with up to 57 devices. When using large tree support, please note the following:

– In the large tree support RSTP topology, **do not** use devices that **do not** support large tree support.
– Enable the large tree support option on **all** devices.
– If RSTP is to be activated as the redundancy mechanism in an existing network with more than seven switches along the relevant path, then the large tree support option must first be enabled on all devices.
– It is recommended that large tree support is not activated in networks with less than seven switches along the relevant path.

Maximum Age of STP Information
The parameter is set by the root switch and used by all switches in the ring. The parameter is sent to make sure that each switch in the network has a constant value, against which the age of the saved configuration is tested.

The "Maximum Age of STP Information", "Hello Time", and "Forward Delay" fields have the same meaning as for STP. These values are used when this switch becomes a root. The values currently used can be found under (R)STP General.

Hello Time
Specifies the time interval within which the root bridge regularly reports to the other bridges via BPDU.

Forward Delay
The forward delay value indicates how long the switch is to wait in order for the port state in STP mode to change from "Discarding" to "Listening" and from "Listening" to "Learning" (2 x forward delay).

The "Maximum Age of STP", "Hello Time", and "Forward Delay" parameters are optimized by default upon delivery. They should not be modified.

(R)STP Port Table

(R)STP Port Table

Module	Interface	Port	Oper Edge Port	Protocol	STP State
HS	X1	1	edge port	RSTP	forwarding
		2	edge port	RSTP	discarding
	X2	3	edge port	RSTP	discarding
		4	edge port	RSTP	discarding
	X3	5	edge port	RSTP	discarding
		6	edge port	RSTP	discarding
	X4	7	edge port	RSTP	forwarding
		8	edge port	RSTP	discarding

Note: This web page will be refreshed in 22 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces)!

Figure 5-5 (R)STP Port Table

Oper Edge Port
All ports that do not receive any (R)STP BPDUs (e.g., termination device ports) become edge ports, i.e. ports that go to the "Forwarding" state immediately after restart.

Protocol
Indicates the redundancy protocol used.

(R)STP State
Indicates the current (R)STP state of the relevant port.

Possible states:

– "Forwarding"
  The port is integrated in the active topology and forwards data.
– "Discarding"
  This port does not take part in data transmission.
– "Learning"
  This port does not take part in data transmission of the active topology, however, MAC addresses are learned.
– Blocking/Discarding
  The port has a link, but has not been set to the "Discarding" state by RSTP.

(R)STP Port Configuration Table

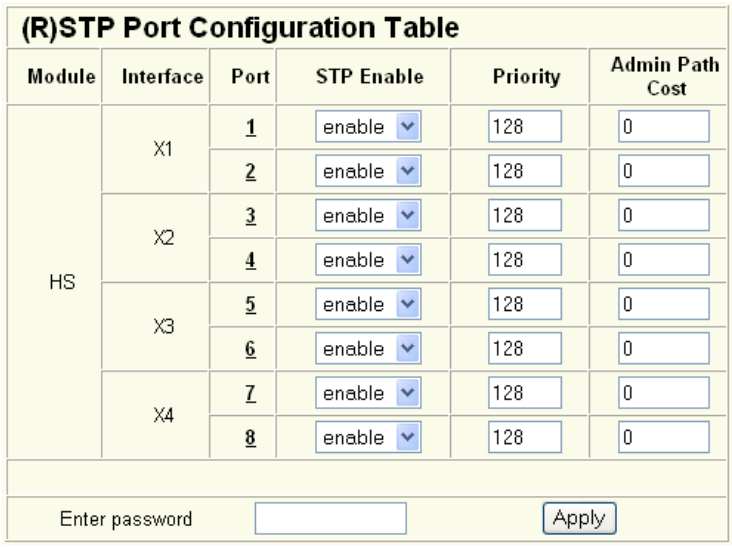


Figure 5-6 "(R)STP Port Configuration Table" menu

An overview of the main settings for each port is provided here:

5.2.1.2 (R)STP Port Configuration

Modifications of properties can result in complete reconfiguration of (Rapid) Spanning Tree.

It is recommended that a suitable root switch and a backup root switch are specified using corresponding priority assignment.

This page displays the valid (R)STP configuration settings for the selected port.

If termination devices or subnetworks are connected without RSTP or STP via a port, it is recommended that the "Admin Edge Port" be set to "Edge Port". In this way, a link modification at this port does not result in a topology modification.

5.2.1.3 Switch/Port ID

The validity of switches and ports is determined according to priority vectors.

Bridge Identifier

A switch ID consists of 8 bytes as an unsigned integer value. When comparing two switch IDs, the one with the lowest numeric value is of higher, i.e., "better" priority.

The first two bytes contain the priority.
The last 6 bytes contain the MAC address and thus ensure the uniqueness of the switch ID in the event of identical priority values.

The switch with the lowest numerical switch ID becomes the root. It is recommended that the root port and alternate port are specified using the priority.

Port Identifier

The port ID consists of 4 bits for the port priority and 12 bits for the port number. The port ID is interpreted as an unsigned integer value. When comparing two port IDs, the one with the lowest numeric value is of higher, i.e., "better" priority.

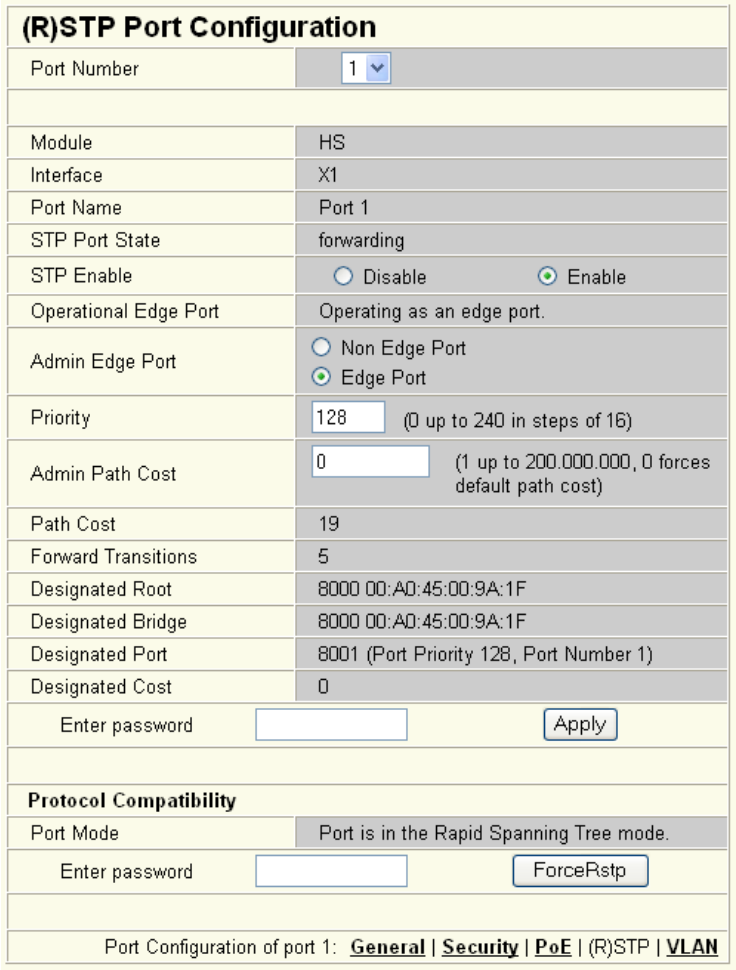


Figure 5-7 (R)STP Port Configuration

Port Number
Indicates the number of the port currently selected.

Port Name
Indicates the name of the port.

STP Port State
Indicates the status in which this port takes part in STP.

Operational Edge Port
Indicates whether this port is operated as an edge port.

Admin Edge Port
Here you can specify whether this port is to be operated as an edge port (default setting), if possible.

Priority
Indicates the priority set for this port (default 128). Due to backwards compatibility with STP, priority values can be set that are not configurable in RSTP.

Admin Path Cost
Indicates the path costs set for this port. A path cost equal to "0" activates the cost calculation according to the transmission speed (10 Mbps = 100; 100 Mbps = 19).

Path Cost
Indicates the path costs used for this port.

Forward Transitions
Indicates how often the port switches from the "Discarding" state to the "Forwarding" state.

Additional parameters provide information about network paths in a stable topology that are used by the BPDU telegrams.

Designated Root
Root bridge for this Spanning Tree.

Designated Bridge
The switch from which the port receives the best BPDUs. The value is based on the priority value in hex and the MAC address.

Designated Port
Port via which the BPDUs are sent from the designated bridge. The value is based on the port priority (2 digits) and the port number.

Designated Cost
It indicates the path costs of this segment to the root switch.

Protocol Compatibility

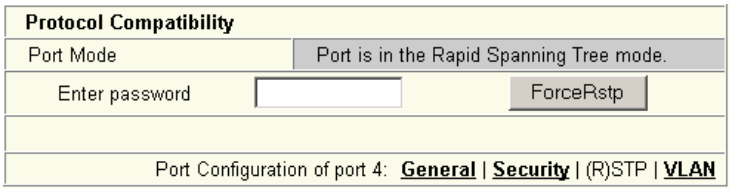

Protocol Compatibility
Port Mode
Port is in the Rapid Spanning Tree mode.
Enter password
ForceRstp
Port Configuration of port 4: General | Security | (R)STP | VLAN

Figure 5-8 Protocol Compatibility

If a port receives STP BPDUs, it switches automatically to STP mode. Automatic switching to (R)STP mode does not take place. Switching to (R)STP mode can only be forced via "Force Rstp" or via a restart.

RSTP Fast Ring Detection

The "RSTP Fast Ring Detection" function can be activated on the "RSTP Configuration" web page (see page 5-5).

This function speeds up the switch-over to a redundant path in the event of an error and provides easy diagnostics. RSTP fast ring detection provides each ring with an ID, this ID is made known to each switch in the relevant ring. A switch can belong to several different rings at the same time.

Structure of the Ring ID

The ring ID consists of the port number of the blocking port and the MAC address of the corresponding switch. Advantages of the ring ID:

– Easier to identify redundant paths and locate blocking ports.
– Possible to check whether the desired topology corresponds to the actual topology.

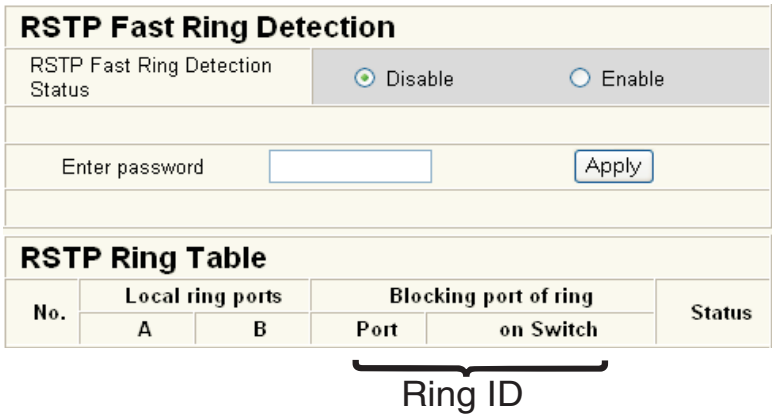


Figure 5-9 RSTP Ring Table

Information in WBM

The following information is displayed on the web page (and via SNMP):

Local Ring Ports
These two ports of this switch belong to the ring that is listed (ring ID).

Blocking Port
This port deliberately breaks the loop.

Ring detection states

The following states can occur for ring detection:

– **Not Ready** - Ring detection has not yet been completed.
– **OK** - Ring detection has been completed and quick switch-over is possible in the event of an error.
– **Breaked** - The ring is broken on this branch in the direction of the root switch.
– Failed on Port A - The ring was broken on this switch at port A.

In the event of a link failure in the ring, the "trapRstpRingFailure" trap is sent.

If "Breaked" or "Failed" status lasts for longer than 60 seconds, it is no longer displayed after the next topology modification, since these rings no longer exist.

When using RSTP fast ring detection, please note the following:

– For RSTP fast ring detection, **do not** use devices that **do not** support this function.
– Enable RSTP fast ring detection on **all** devices.
– All data paths must be in full duplex mode.

5.2.2 Connection Failure - Example

The following diagram illustrates an RSTP ring with six switches, where switch 1 is the root. The ring extends over port 1 and port 2 for each switch. On switch 4, the loop is broken by a blocking port.

If a cable interrupt occurs at the point indicated by the star, this produces the following entries on the "RSTP Fast Ring Detection" web page:

Switch 3 - Failed on Port A

Switch 4 - Broken

Switch 3 would also generate the "flWorkLinkFailure" trap, as long as the sending of traps is not disabled.

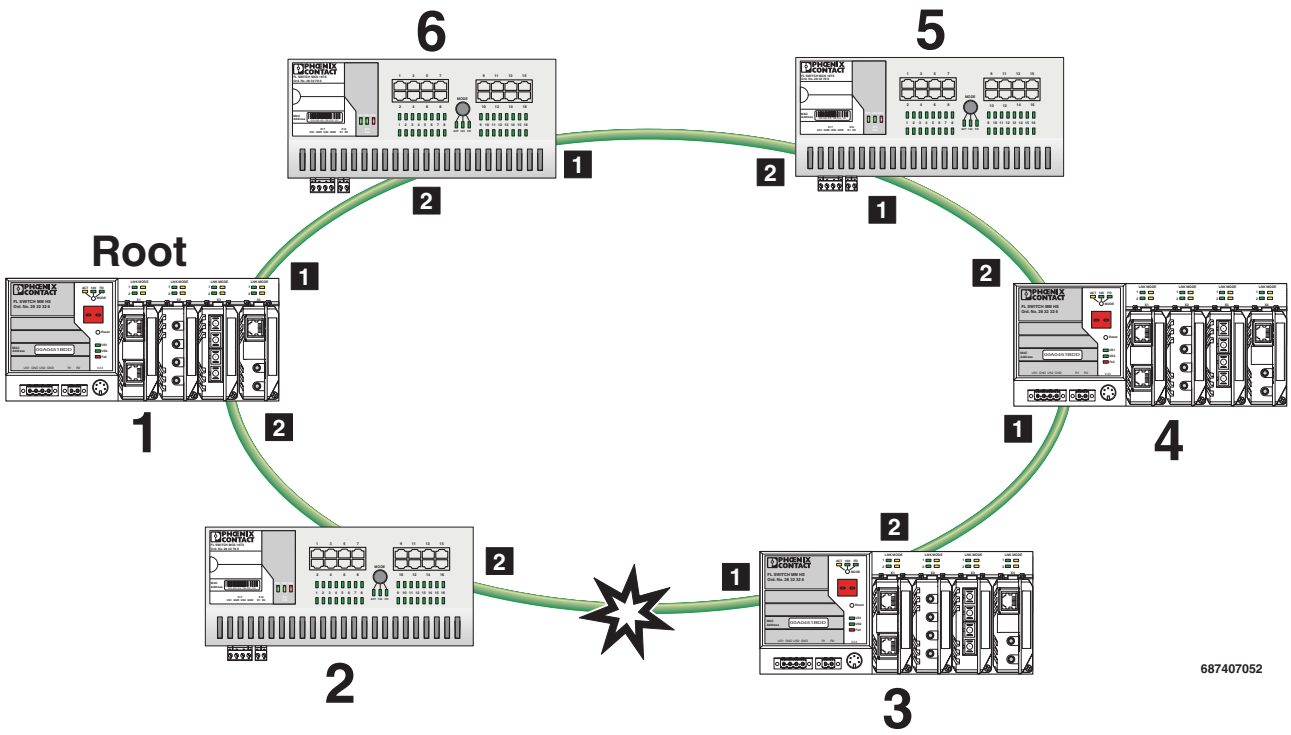


Figure 5-10 Connection failure with RSTP ring detection

5.2.3 Mixed Operation of RSTP and STP

If a device with STP support is integrated into the network, only switch ports that receive STP BPDUs are set to STP mode. All other ports that receive RSTP BPDUs remain in RSTP mode.

5.2.4 Topology Detection of a Rapid Spanning Tree Network (RSTP)

(Rapid) Spanning Tree switches continually exchange information about the network topology using special messages (BPDUs - Bridge Protocol Data Units). In this way the switches "learn" the current network topology and - based on this information - make the following decisions:

– Which switch is selected as root switch
– Which data paths are disabled

If a switch is started using the (Rapid) Spanning Tree Protocol, it first expects to be the root switch. However, no data communication is possible during the startup phase until the current network topology has been learned and until the decisions described above have been made. Therefore loops which could otherwise occur during the network startup phase because no data path is interrupted, are prevented.

5.2.4.1 Topology Modification

A topology modification can be triggered by the following:

– Adding a data path
– Failure of a data path
– Adding a Spanning Tree switch
– Failure of a Spanning Tree switch

A topology modification is automatically detected and the network is reconfigured so that another tree is created and all the devices in this tree can be accessed. During this process, loops do not even occur temporarily.

If the sending of traps was not deactivated, two traps are generated:

– newRoot (OID: 1.3.6.1.2.1.17.0.1)
– topologyChange (OID 1.3.6.1.2.1.17.0.2)

5.2.4.2 Interrupted Data Paths and Port States

The described data path interruption by the Spanning Tree Protocol is created by disconnecting individual ports that no longer forward any data packets. A port can have the following states:

– Learning
– Forwarding
– Blocking/Discarding
– Disabled (link down or disconnected by the user)

The current port states are shown in the web interface.

The properties of the various port states are shown in the table below.

Table 5-1 Properties of the port states

	Receiving and Evaluating BPDUs (Learning the Topology)	Learning the MAC Addresses of Connected Devices and Creating Switching Tables	Forwarding Data Packets (Normal Switching Function)
Disabled			
Blocking/Discarding	X		
Learning	X	X	
Forwarding	X	X	X

The sequence of the five port states defined in the Spanning Tree Protocol cannot be assigned freely. The following diagram illustrates the possible sequence of the port states.

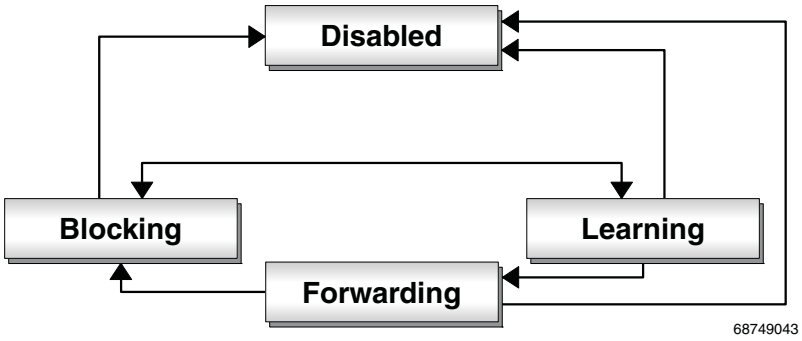


Figure 5-11 Sequence of the possible port states in STP

After device startup and, if necessary, also during topology modification, a port passes through the states in the following order:

Learning → Forwarding

Or

Disabled → Blocking/Discarding

Due to the edge property of ports, they switch to "Forwarding" immediately. In the second case, the port generates a data path interruption in order to suppress loops accordingly.

At least one port in the "Forwarding" state is at a data path between two Spanning Tree switches so that the data path can be integrated into the network.

5.2.4.3 Fast Forwarding

If the Spanning Tree Protocol is deactivated at a port, the corresponding port is in "Fast Forwarding" mode.

A fast forwarding port:

– Ignores all BPDUs that are received at this port.
– Does not send any BPDUs.

– Switches to the "Forwarding" state immediately after establishing the data link. Termination devices connected to this port can be accessed immediately.

"Port STP Status" in WBM on the "STP Port Configuration" page must be set to "Disabled" to activate fast forwarding.

Frame duplication

Due to the fast switch-over times of RSTP, frames may be duplicated and the order of frames may be changed.

5.2.4.4 Enabling via Serial Interface or Telnet

Establish a connection to the switch as described in "Management via Local V.24 (RS-232) Communication Interface" on page 4-116 or "Management via Telnet" on page 4-123. Set "Spanning Tree, Enabled" on the following page in the "Redundancy" field and select "Save".

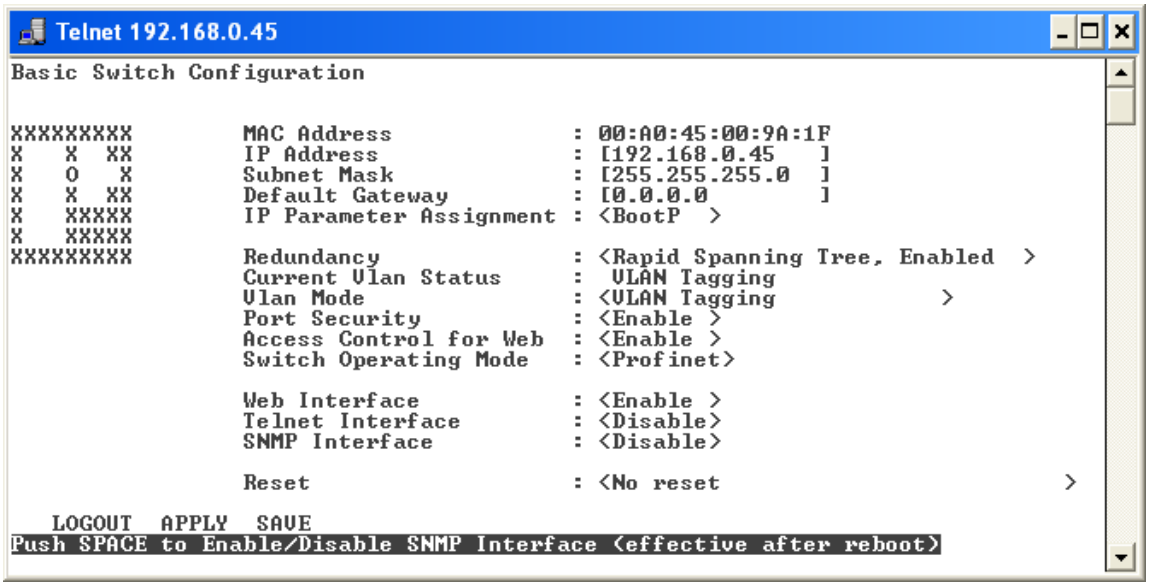


Figure 5-12 Activating Rapid Spanning Tree

5.2.5 Configuration Notes for Rapid Spanning Tree

In contrast to the Spanning Tree method, the Rapid Spanning Tree method supports event-controlled actions that are no longer triggered based on a timer.

If one cable fails (link down), the Rapid Spanning Tree method can respond more quickly to this failure and thus the switch-over time can be kept low.

A link down or link up must be detected at the switch so that the RSTP switches can detect a line failure and a restored line more quickly. Please take into consideration, in particular, paths where media converters are used. If required, media converters offer setting options to transmit the link status of the fiber optic side to the twisted pair side.

If a link down is not detected at the switch, due to the cable interrupt between the media converters, and if no link down is forced at the switch, timer-based detection is activated, which may result in longer switch-over times.

– For short switch-over times, structure your network in such a way that a maximum of seven switches are located in a cascade up to the root switch. The switch-over times can range from 100 ms to 2 s.
– Use priority assignment to specify a central switch as the root.
– It is also recommended to assign a switch as the backup root.
– For short switch-over times, all switches in the redundant topology should support the Rapid Spanning Tree Protocol and should not use hubs.

5.2.5.1 Connecting the Switches to Form a Meshed Topology

Having activated (Rapid) Spanning Tree for all switches, you can create a meshed topology with redundant data paths. Any data connections can now be created without taking loops into consideration. Loops can even be added on purpose in order to create redundant connections.

A data path between Spanning Tree switches can be:

– A direct connection.
– A connection via one or more additional switches that do not support Spanning Tree.

If Spanning Tree is not supported by all of the switches used, the reconfiguration time for Spanning Tree is extended by the aging time of switches without Spanning Tree support.

– A connection via one or more additional hubs that do not support Spanning Tree.

Furthermore, a data path can also consist of a connection of a Spanning Tree switch to:

– A termination device.
– A network segment in which **no** loops may occur, which consists of several infrastructure components (hubs or switches) without Spanning Tree support.

For the last two data path options, no specific precautionary measures are necessary. If necessary, the "Fast Forwarding" option can be used for the relevant ports (see "Fast Forwarding" on page 5-13).
For the first three cases, the following rules must be observed:

– **Rule 1: Spanning Tree transparency for all infrastructure components**
  All infrastructure components used in your network that do not actively support Spanning Tree must be transparent for Spanning Tree messages (BPDUs) and must forward all BPDUs to all ports without modifying them. When Spanning Tree is disabled, the switch is transparent for BPDUs.

– **Rule 2: At least one active Spanning Tree component per loop**
  An active Spanning Tree component supports the Spanning Tree Protocol, sends/receives and evaluates BPDUs, and sets its ports to the relevant STP states. Each loop in a network must have at least one active Spanning Tree component to disintegrate the loop.
  Example:

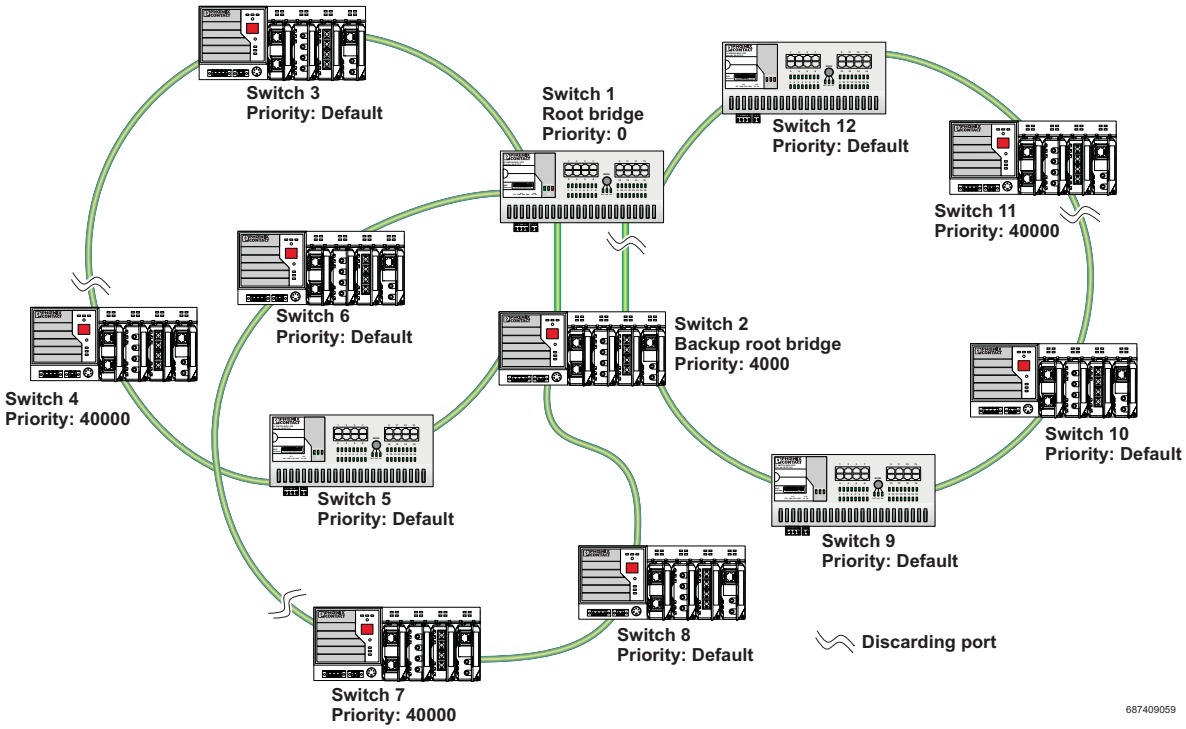


Figure 5-13 Example topology

The loops in the example topology illustrated are disabled by active RSTP components. The example topology contains three rings, the root and the backup root are components in each of the three rings. The three rings do not affect one another, a modification to the topology in one ring does not affect the topology of the other two rings.

– **Rule 3: No more than ten active Spanning Tree components in the topology when using Spanning Tree default settings**
  The ability to disintegrate any topology to form a tree without loops requires a complex protocol that works with several variable timers. These variable timers are

dimensioned using IEEE standard default values so that a topology with a maximum of ten active Spanning Tree components always results in a stable network. When using large tree, please note the following (see also "Large Tree Support" on page 5-5):

– In the large tree support RSTP topology, **do not** use devices that **do not** support large tree support.
– Enable the large tree support option on **all** devices.
– If RSTP is to be activated as the redundancy mechanism in an existing network with more than seven switches along the relevant path, then the large tree support option must first be enabled on all devices.
– It is recommended that large tree support is not activated in networks with less than seven switches along the relevant path.

5.2.5.2 Example Topologies

5.2.5.3 Redundant Coupling of Network Segments

In this example, two network segments are connected via redundant data paths. Two RSTP components have ports in the "Blocking/Discarding" state (highlighted in gray). This is sufficient to operate the network.

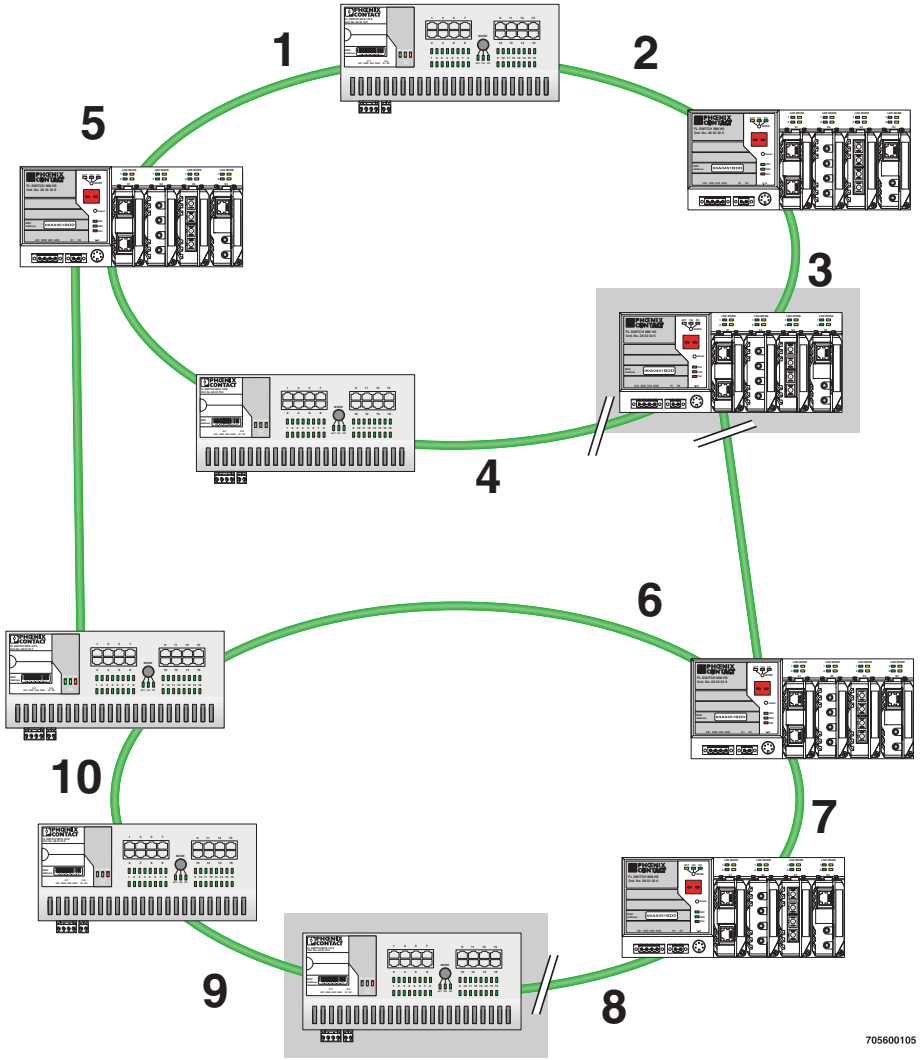


Figure 5-14 Redundant coupling of network segments

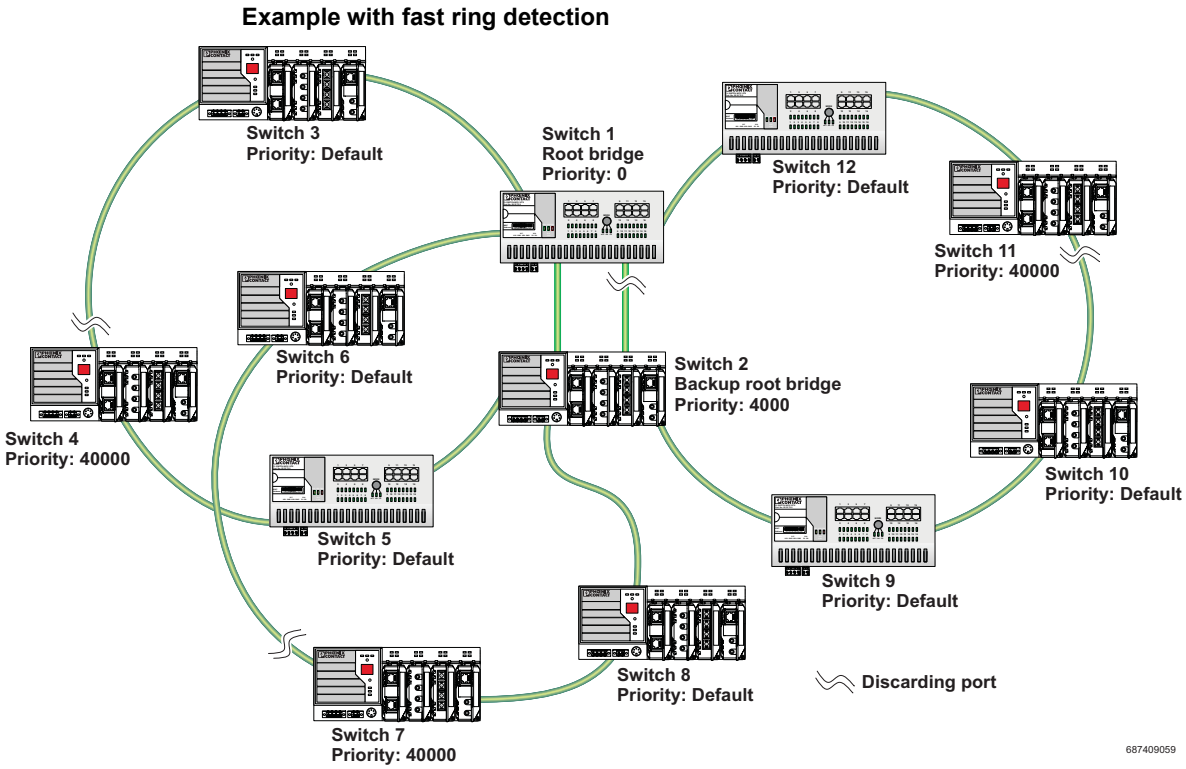


Figure 5-15 Example with fast ring detection

The switches in the illustrated example are arranged in such a way that two devices at the central position are configured as the root bridge and as the backup root bridge (via the priority).

The root bridge has the lowest priority, the backup root bridge has the second lowest priority. The root and the backup root bridge are connected together redundantly. The remaining switches are networked in several rings in a ring topology. The end points of the ring are implemented on the root bridge and on the backup root bridge. The switch furthest away from the root bridge has a low priority as its default setting, e.g., 40000.

The advantage of this constellation is that the individual rings are not adversely affected in the event of an error.

5.2.5.4 Method of Operation of the Spanning Tree Protocol (STP)

Components of a Spanning Tree Domain

Designated Switch

The switch that connects a specific LAN segment (with the lowest path costs) to the root switch.

Root Port

The other switches set the port with the lowest path costs (or with the highest total transmission speed) as the root switch in the forwarding state.

There is only ever one root port per switch.
Exception: The switch supports several Spanning Tree domains.

Designated Ports

Ports in the forwarding state of the designated switch.
These are the ports with the "best" path to the root switch.

Switch ID

Priority and MAC Address

The switch with the lowest bridge identifier is the root switch. The bridge identifier consists of the MAC address and the priority. Since the priority appears before the MAC address, the appropriate priority can be clearly assigned by the root switch, independent of the MAC address. The switch with the highest priority (lowest value) becomes the root switch.
For every switch port within the network, a unique cost calculation is created. These root path costs are the sum of all path costs for one packet on the path between the root switch and corresponding switch port. The port of a switch with the lowest root path costs is always the active port. If the same root path costs have been calculated for two or more ports, the switch priority followed by the port priority determine the priority of the path.

Port ID

The port identifier consists of the path costs and the priority. Since the priority appears before the path costs, the appropriate priority can be clearly assigned by the root switch, independent of the path costs. The port with the highest priority (lowest value) becomes the root port.

5.2.5.5 Processes in the Spanning Tree Protocol (STP)

Selecting the Root Switch

On every topology modification, each switch first assumes that it is the root switch and thus sends its own switch ID (e.g., the MAC address) into the network. All switches receive these messages (MAC multicast) and store the contents of the "best" message. The "best" message consists of the following topology information: the root ID information and the cost information.

Having received the root ID information, the switch compares the following:

– The new root ID is saved if it has a higher priority than the IDs that are already saved (including its own ID).
– The path costs are checked if the root ID is the same as the one already saved. If they are lower, the ID is saved.
– If the root ID and the costs are the same, the ID of the sender is checked. If the ID is lower than the switch's own ID, it is saved.
– If the root ID, costs, and sender ID are the same, the priority of the sender port is the decisive criterion.

Selecting a Designated Switch

For every network the switch with the most favorable root connection is selected, this switch is called the designated switch.
The root switch is the designated switch for all directly connected networks.

Selecting a Root Port

Once the root switch has been specified by processing the root IDs, the switches now specify the root ports.

The most favorable path is specified by minimizing all connection costs on the path to the root switch. In addition, transmission speeds can also serve as costs. For the switch, the path costs added by each port for every HOP (the hop of a data packet from one point to the next) are preset to a value of 19 (default setting/recommended for 100 Mbps) and can be modified at any time by the user.

Selecting a Designated Port

At every "designated switch" the port with the most cost-effective data connection in the direction of the root switch is called the designated port.

Port Costs

The port costs can be set according to two different standards, 802.1D (STP) or 801.1W (RSTP).

If, in addition to Phoenix Contact devices, devices from other manufacturers are also used, it is recommended that the port costs are set according to a uniform standard.

The "dot1dstpPathCostDefault" SNMP object (OID 1.3.6.1.2.1.17.2.18) can be used to change the standard that is used.

Table 5-2 Port costs according to 802.D

Transmission Speed	Recommended Value	Recommended Range
10 Mbps	100	50 - 600
100 Mbps	19	10 - 60

Table 5-3 Port costs according to 802.W

Transmission Speed	Recommended Value	Recommended Range
10 Mbps	2,000,000	200,000 - 20,000,000
100 Mbps	200,000	20,000 - 2,000,000

5.2.5.6 Flowchart for Specifying the Root Path

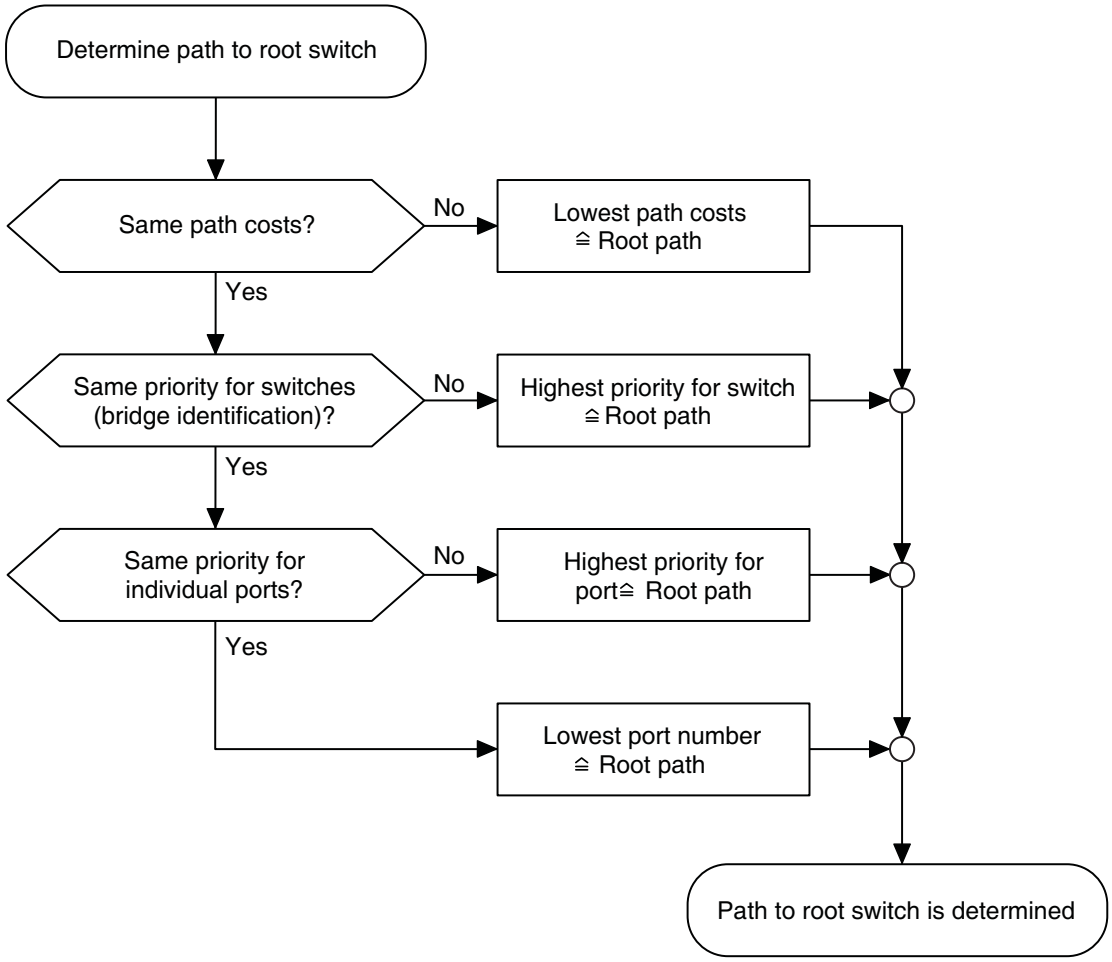


Figure 5-16 Flowchart for specifying the root path

5.2.5.7 Extended Configuration

It may be useful to actively specify the topology that is formed due to the Spanning Tree Protocol and to not leave it to the random MAC addresses of the switches involved. Non-blocking/blocking data paths can thus be influenced and a load distribution specified.
It may also be useful to explicitly disable the Spanning Tree Protocol at ports that do not participate in Spanning Tree so as to benefit from the fast forwarding function.
The Spanning Tree Protocol must also be disabled at individual ports if two different network segments - both using Spanning Tree - are to be coupled via these ports without the two tree structures merging into a large Spanning Tree.

Specifying the Root Switch

The root switch is assigned via the assignment of an appropriate priority for the Spanning Tree segment. Set the highest priority (lowest value) in the "Priority" field on the "STP Bridge Configuration" page in WBM for the switch selected as the root switch. Make sure that all the other network switches have a lower priority (higher value). Here, the set path costs are not evaluated.

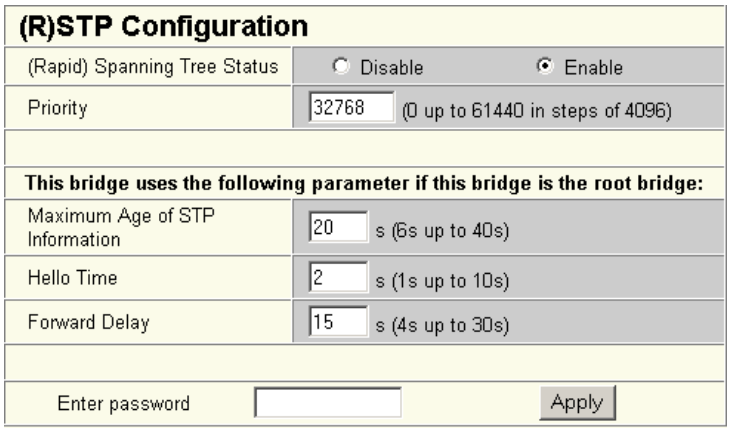


Figure 5-17 Specifying the root switch priority

Specifying the Root Port or Designated Port

The root port and designated port are always the ports with the lowest path costs. If the costs are the same, the priority is the decisive criterion. If the priorities are also the same, the port number is the decisive criterion. Specify an appropriate combination of costs and priority on the "STP Port Configuration" page in WBM for the port specified as the root port or designated port. Make sure that all the other network switches either have higher costs or a lower priority (higher value).

5.2.5.8 Disabling the Spanning Tree Protocol/Using the Fast Forwarding Function

One of the following requirements must be met so that the Spanning Tree Protocol can be disabled for a port:

– A termination device is connected to the port.
– Additional infrastructure components are connected to the port. The corresponding network segment does not contain any loops.
– Additional infrastructure components are connected to the port, forming a Spanning Tree of their own. No additional redundant connections to this network segment are permitted.

5.2.5.9 Modifying the Protocol Timer

Modifying the protocol timer may result in unstable networks.

It may be necessary to modify the protocol timer if, e.g., there are more than ten active Spanning Tree components in a single network. You can also attempt to reduce the reconfiguration times by modifying the timer. However, care should be taken in order to prevent unstable networks.
Please note that the protocol times are specified by the root switch and that they are distributed to all devices via BPDU. It is therefore only necessary to modify the values in the root switch. If the root switch fails, the timer values of another active STP switch (i.e., the new root switch) will be valid for the entire network segment. Please remember this during component configuration.

Specifying the Timer Values (STP and RSTP)

– Maximum number of active Spanning Tree components along the path beginning at the root switch (please refer to the following two example illustrations):
= (MaxAge/2) - Hello Time + 1
– 2 x (Forward Delay - 1 s) ≥ MaxAge
– MaxAge ≥ 2 × (Hello Time + 1 s)

The value ((MaxAge/2) - Hello Time) for a ring topology corresponds to the maximum number of components with active Spanning Tree.

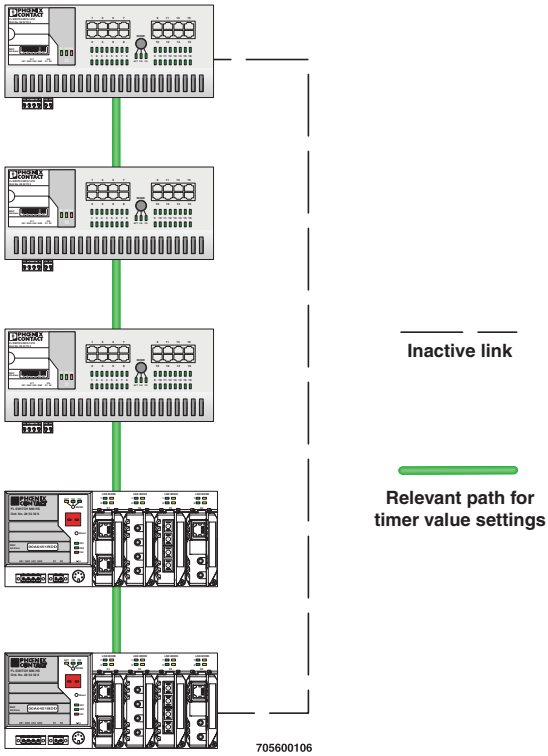


Figure 5-18 Example 1 for the "relevant path"

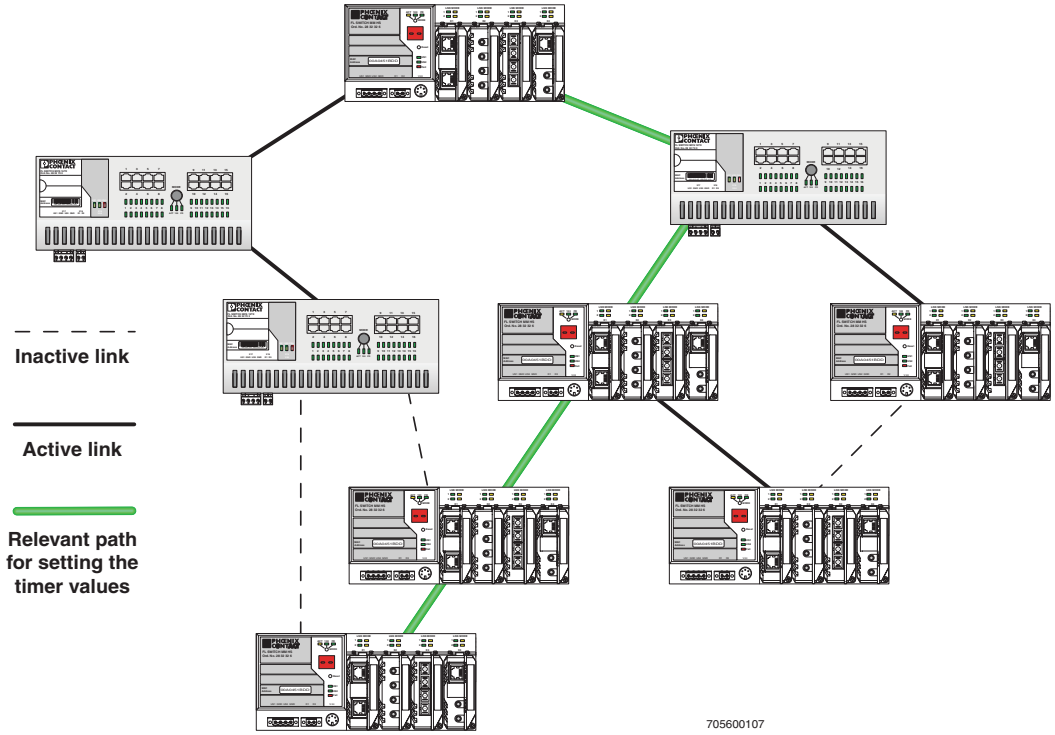


Figure 5-19 Example 2 for the "relevant path"

5.2.5.10 Reconfiguration Times

The reconfiguration time for a Spanning Tree depends on the timer values for MaxAge and Forward Delay.

The minimum reconfiguration time is:
2 × Forward Delay

The maximum reconfiguration time is:
2 × Forward Delay + MaxAge

For the values recommended by the IEEE standard, the value for ten active STP switches along a path beginning with the root switch is between 30 s and 50 s.

Switch-Over Time Response to Be Expected for RSTP and RSTP With Activated Ring Detection

When using **RSTP**, expect switch-over times in the range from **100 ms to 2 s**.

When using **fast ring detection**, expect switch-over times in the range from **100 ms to 500 ms**.

Port Roles

The **root port** of a switch connects this switch to the root switch - either directly or via another switch (designated switch).

The **designated port** is the port at a designated switch that is connected to the root port of the next switch.

No additional switches/bridges are connected to **edge ports**. Termination devices are connected to edge ports.

An **alternate port** is a path to the root, which, however, did not become a root port. I.e., this port is not part of the active topology.

6 Multicast Filtering

6.1 Basics

Multicast

Multicast applications, unlike unicast applications with point-to-point communication, do not transmit their data with the MAC address of the destination, but with an independent multicast group address. Always using connectionless communication, a station transmits **one** data packet that is received by one or more receiver stations.

Advantages:

1. If, for example, a data packet of a transmitter is to be transmitted to eight receivers, the same packet does not have to be sent eight times to the addresses of all eight devices. Instead it only needs to be sent once to the address of the multicast group that includes the eight devices.
2. When using multicast communication and filtering, the required bandwidth for data transmission is reduced because each packet can only be transmitted once.

A maximum of 20 multicast groups can be created.

6.2 Enabling the Web Pages for Multicast Filtering in WBM

Activate WBM for the switches, e.g., using the Factory Manager. Switch to the "General Configuration" menu, then the "User Interfaces" page. Activate "Multicast Filtering" and confirm by entering your password.

When activating "Multicast Filtering" under "General Configuration/User Interfaces", the multicast mechanism is **not** activated. In the WBM menu, the "Multicast" page - under which the function can be configured and activated - is enabled.

6.3 Static Multicast Groups

Static multicast groups must be created manually on every switch and all ports that are used to contact group members need to be added. The advantages of static groups are:

1. Easy specification of network paths on which the multicast data traffic of known groups is limited.
2. No querier required (see "Query" on page 6-7).

The following marginal conditions must be observed:

– Precise network documentation for path specification is required.
– Possible redundant paths due to Spanning Tree must be taken into account during port assignment.

– For network modifications, during servicing or expansion, the multicast data paths must be restored.

6.3.1 "Current Multicast Groups" Web Page

The table on this web page provides an overview of the current multicast groups created on this MMS. These include multicast groups that are assigned as a result of IGMP snooping or groups that are statically created.

Current Multicast Groups

VID	Group Address	Group	Membership
1	01:00:5e:00:18:08	Ports 1-8	☐ ☐ ☑ ☑ ☐ ☐ ☐ ☐
1	01:00:5e:00:19:21	Ports 1-8	☑ ☐ ☐ ☐ ☐ ☑ ☑ ☑
3	01:00:5e:00:18:2d	Ports 1-8	☑ ☑ ☐ ☐ ☐ ☐ ☐ ☐
7	01:00:5e:00:a8:a8	Ports 1-8	☐ ☑ ☐ ☐ ☑ ☐ ☑ ☐

Note: This web page will be refreshed in 15 sec automatically (change the interval at the web page 'Services')!

Figure 6-1 "Current Multicast Groups" web page

These checkboxes indicate which port has been assigned to each individual group.

Please note that all multicast groups that are known to the switch, including the dynamically detected groups that have not been created manually, are shown on this web page.

The overview for group membership is based on the "dot1qTpGroupTable" SNMP group. This table contains all groups (static entries and IGMP) and their members.

6.3.2 Creating Static Multicast Groups

This web page is used to create and manage statically configured multicast groups. In order to create a multicast group, enter the MAC address provided (see "Multicast Addresses" on page 6-4) for the multicast group in the "Multicast Group Address" field, add the ports of the data paths to the group members, and confirm these entries by entering a valid password. If a group address is entered as an IP address, the IP address is converted into a multicast MAC address according to the specifications of IEEE 802.1 D/p.

Overwriting a dynamic group with a static configuration means that a new port assignment for this group cannot be created dynamically. Only deleting this group will enable port assignment for this group to be started dynamically.

Conversion

The guidelines for converting multicast IP addresses into a multicast MAC address results in the mapping of different IP groups to the same MAC group. Avoid the use of IP groups:

– That do **not** differ in the **first and second byte** from the right
– That differ by 128 in the **third byte** from the right

The **fourth byte** from the right is always replaced by 01:00:5e during conversion. See example below:

Because of the conversion from IP to MAC addresses, you should avoid using IP addresses that differ with regard to the third byte from the right by 128. Example:

	3rd byte from the right	
1st multicast IP address:	228 . 30	. 117 . 216
2nd multicast IP address:	230 . 158	. 117 . 216
Difference:	128	

Both multicast IP addresses are converted into the multicast MAC address 01:00:5e:1e:75:d8.

The group is added to the list of existing static multicast groups. This list, which is displayed in a list box, is referred to as "dot1qStaticMulticastTable" in SNMP.

Settings are not automatically saved permanently. The active configuration can be saved permanently by selecting "Save current configuration" on the "Configuration Management" web page.

Port assignment

After entering a new group in the "Multicast Group Address" field, add the ports of the group members by selecting the corresponding checkboxes. Confirm by entering your password and clicking on "Apply".

Modifying assignment

Select the corresponding group in the "Select Group" list box to modify or delete the port assignment. The group members are indicated by activated checkboxes and can be modified, if required. An action is completed by entering a password and clicking on "Apply" or "Delete".

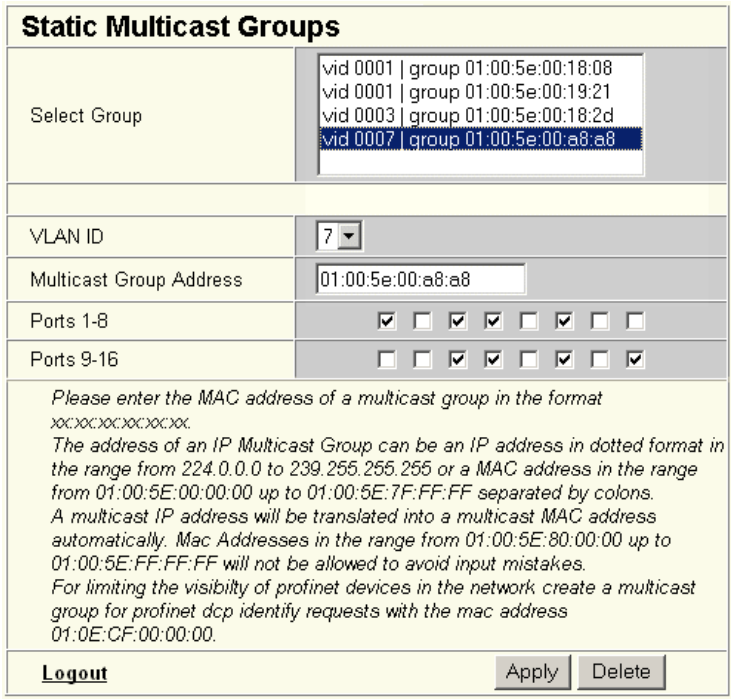

Static Multicast Groups
Select Group
vid 0001 | group 01:00:5e:00:18:08
vid 0001 | group 01:00:5e:00:19:21
vid 0003 | group 01:00:5e:00:18:2d
vid 0007 | group 01:00:5e:00:a8:a8
VLAN ID
7
Multicast Group Address
01:00:5e:00:a8:a8
Ports 1-8
Ports 9-16
Please enter the MAC address of a multicast group in the format xx:xx:xx:xx:xx:xx.
The address of an IP Multicast Group can be an IP address in dotted format in the range from 224.0.0.0 to 239.255.255.255 or a MAC address in the range from 01:00:5E:00:00:00 up to 01:00:5E:7F:FF:FF separated by colons.
A multicast IP address will be translated into a multicast MAC address automatically. Mac Addresses in the range from 01:00:5E:80:00:00 up to 01:00:5E:FF:FF:FF will not be allowed to avoid input mistakes.
For limiting the visibilty of profinet devices in the network create a multicast group for profinet dcp identify requests with the mac address 01:0E:CF:00:00:00.
Logout
Apply
Delete

Figure 6-2 "Static Multicast Groups" menu

Checking group assignment

In order to check which ports are assigned to which group, select one of the existing groups. The corresponding MAC address is then displayed in the "Multicast Group Address" text field. The members of the group are indicated by the activated checkboxes.

Multicast Addresses

Do not use multicast MAC addresses that are in the range from 01:00:5e:80:00:00 to 01:00:5e:FF:FF:FF.

Incorrect format

An incorrect MAC address format and the entry of "non-multicast addresses" is indicated and the entry is not permitted.

Please note that in multicast MAC addresses the bytes are separated by a colon (:) and IP multicast addresses are separated by a full stop (.).

6.3.3 Procedure for Creating a Multicast Group

Gain an overview of the multicast applications available within the network and the multicast addresses used. Create a group for every multicast application or for the multicast address used, and for **each** switch add the ports to which a device of the appropriate group is directly connected or via which the device can be accessed.

Example

In the following table, the ports (for each switch) to which the relevant receivers of the multicast data are connected are indicated with an "X". See example configuration Figure 6-3 on page 6-6.

Table 6-1 Multicast port assignment to the switches

	Switch 1	Switch 2	Switch 3	Switch 4	Switch 5	Switch 6	Switch 7
Port 1							
Port 2	X	X	X	X	X	X	X
Port 3							
Port 4					X		X
Port 5				X			
Port 6						X	
Port 7	X						
Port 8			X		X		

Please note that possible redundant paths must be taken into consideration when using Rapid Spanning Tree for multicast group creation.

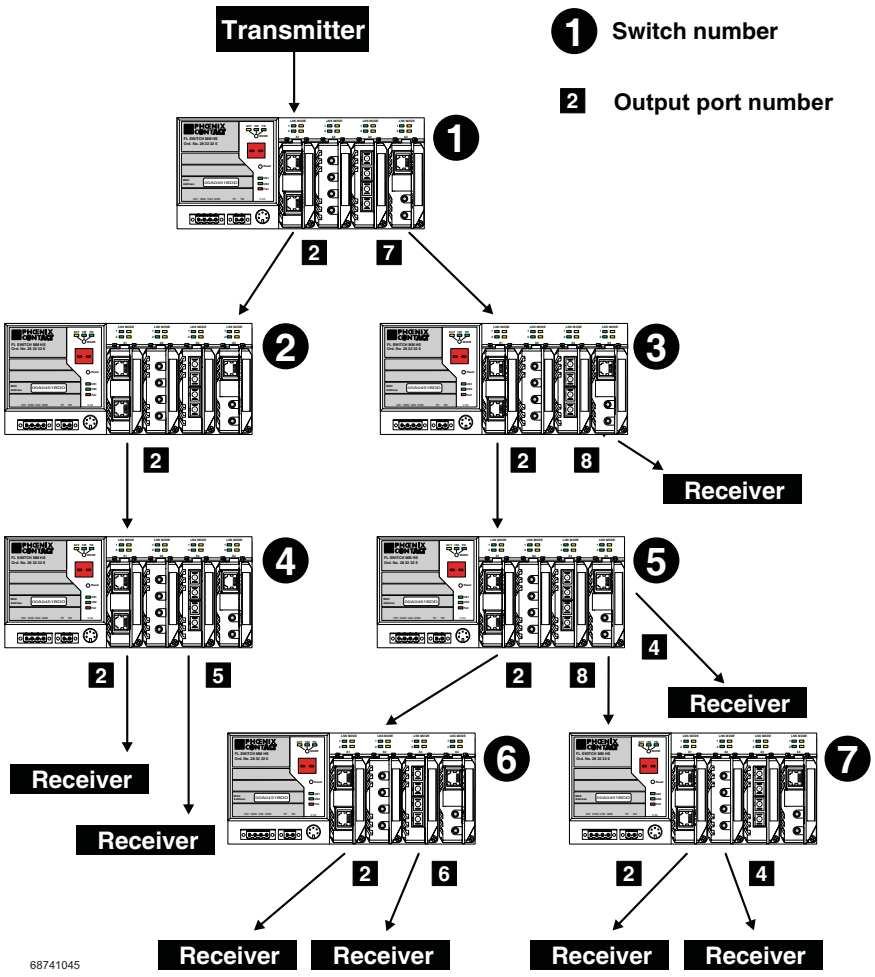


Figure 6-3 Configuration example

Possible redundant paths must be taken into consideration when using Rapid Spanning Tree for multicast group creation.

6.4 Dynamic Multicast Groups

6.4.1 Internet Group Management Protocol (IGMP)

IGMP on Layer 3

The Internet Group Management Protocol describes a method for distributing information via multicast applications between routers and termination devices at IP level (Layer 3).

When starting a multicast application, a network device transmits an IGMP membership report and thus informs its members of a specific multicast group. A router collects these membership reports and thus maintains the multicast groups of its subnetwork.

Query

At regular intervals, the router sends IGMP queries. This causes the devices with multicast receiver applications to send a membership report again.

The "IGMP Query" function only transmits in the management VLAN and only stops if there is a better querier in the management VLAN.

The router enters the IP multicast group address from the report message in its routing table. This means that frames with this IP multicast group address in the destination address field are only transferred according to the routing table. Devices that are no longer members of a multicast group log out with a leave message (IGMP Version 2 or later) and no longer send report messages.
The router also removes the routing table entry if it does not receive a report message within a specific time (aging time). If several routers with active IGMP query function are connected in the network, they determine among themselves which router performs the query function. This depends on the IP address, as the router with the lowest IP address continues to operate as the querier and all the other routers no longer send query messages. If these routers do not receive a new query telegram within a specific period of time, they themselves become queriers again. If there are no routers in the network, a suitably equipped switch can be used for the query function. Please note that the MMS only operates as the IGMP querier in the management VLAN.

IGMP snooping

A switch, which connects a multicast receiver with a router, can read and evaluate IGMP information using the IGMP snooping method. IGMP snooping translates IP multicast group addresses into multicast MAC addresses, so that the IGMP function can also be detected by Layer 2 switches. The switch enters the MAC addresses of the multicast receivers, which were obtained from the IP addresses by IGMP snooping, in its own multicast filter table. Thus the switch filters multicast packets of known multicast groups and only forwards packets to those ports to which corresponding multicast receivers are connected.

IGMP snooping can only be used on Layer 2 if all termination devices send IGMP messages. The IP stack of multicast compatible termination devices with applications linked to a multicast address automatically sends the relevant membership reports.

IGMP snooping operates independently of the Internet Group Management Protocol (IGMP).

6.4.1.1 Extended Multicast Filtering

If IGMP snooping is active, multicast data streams are also detected for which no membership reports of possible recipients are registered. For these multicasts, groups are created dynamically. These multicasts are forwarded to the querier, i.e., the querier port is entered in the group.

If the switch itself is the querier, these multicasts are blocked.

6.4.2 "General Multicast Configuration" Web Page

This web page provides global settings for multicast support. Here, IGMP snooping can be activated and an aging time can be specified for IGMP snooping information.

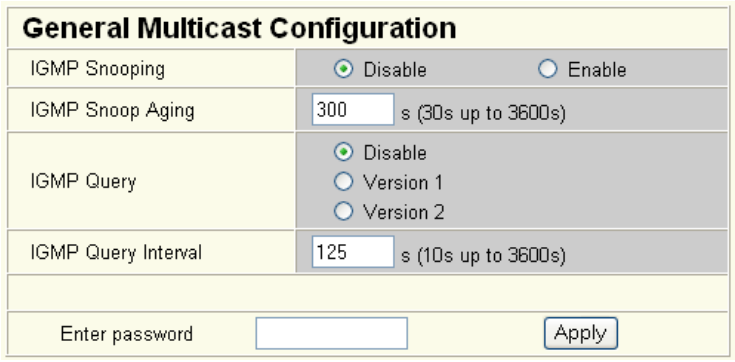


Figure 6-4 "General Multicast Configuration" web page

IGMP Snooping
In IGMP snooping, the switch passively listens in on the IGMP messages that are sent over the network and dynamically creates the appropriate groups. The groups are not saved and will be lost on every power down or when switching off the snooping function.

IGMP Query
An MMS with activated query function actively sends queries at "query intervals" and evaluates the received reports. The MMS only sends IGMP query reports if IGMP snooping is enabled and only in the management VLAN.

7 Virtual Local Area Network (VLAN)

7.1 Basics

VLAN

A VLAN is a closed network, which is separated logically/functionally rather than physically from the other networks. A VLAN creates its own broadcast and multicast domain, which is defined by the user according to specified logical criteria. VLANs are used to separate the physical and the logical network structure.

– Data packets are only forwarded within the relevant VLAN
– The members of a VLAN can be distributed over a large area

The reduced propagation of broadcasts and multicasts increases the available bandwidth within a network segment. In addition, the strict separation of the data traffic increases system security.

A router or similar Layer 3 device is required for data traffic between VLANs.

For the switch, the VLANs can be created statically or dynamically. For dynamic configuration, the data frames are equipped with a tag. A tag is an extension within a data frame that indicates the VLAN assignment. If configured correspondingly, this tag can be added or removed again from the last tag during the transmission of the first switch in the transmission chain. Several different VLANs can thus use the same switches/infrastructure components. Alternatively, termination devices that support VLAN tags can also be used.

7.2 Enabling the VLAN Web Pages in Web-Based Management

Activate web-based management for the switches, e.g., using the Factory Manager, switch to the "General Configuration" menu, then the "User Interfaces" page. Activate the "VLAN" function and confirm by entering your password.

When activating "VLAN" under "User Interfaces", the VLAN mechanism is **not** activated. In the WBM menu, the "VLAN" page - under which the function can be configured and activated - is enabled.

When deactivating the VLAN configuration pages under "User Interfaces", the VLAN mechanism is **not** deactivated. The saved VLAN configuration is retained.

7.2.1 Management VLAN ID

The management of the switch is assigned to VLAN 1 by default upon delivery. In addition, all ports are assigned to VLAN 1 by default upon delivery. This ensures that the network-supported management functions can be accessed via all ports.

Make sure that the MMS is always managed in a VLAN that you can also access.

VLAN ID 1 cannot be deleted and is thus always created on the switch.

If you delete the VLAN in which the MMS is managed, management is automatically switched to VLAN 1.

The "IGMP Query" function only transmits in the management VLAN and only stops if there is a better querier in the management VLAN.

7.2.2 Changing the Management VLAN ID

7.2.2.1 Configuration in Transparent Mode

1. In WBM, enable the pages for VLAN configuration (WBM: User Interfaces/Virtual LAN).
2. Create the required VLANs on the "Static VLANs" web page.
3. On the "VLAN Port Configuration Table" web page, assign the ports for incoming packets to individual VLANs using the VLAN ID.
4. On the "IP Configuration" web page, the desired management VLAN ID can now be set.
5. On the "General VLAN Configuration" web page, set the switch to "Tagging" VLAN mode.
6. Save the configuration on the "General Configuration/Configuration Management" web page and restart the switch.

7.2.2.2 Configuration in Tagging Mode (Usually Used to Change the Management VLAN ID in the Event of an Existing VLAN Configuration)

1. Connect the PC directly to the switch to be configured via a port (A) whose VLAN ID is set to "1".
2. Update the firmware to Version 4.03 or later and restart the switch.
3. Place another port (B) in the desired management VLAN. Port B must be an "untagged member" of the desired management VLAN. Set the corresponding port VLAN ID, if necessary.
4. Set the desired VLAN ID as the management VLAN.
5. Connect your PC to the switch via port B and save the configuration.

7.3 General VLAN Configuration

Basic settings for VLAN operation can be made on the "Switch Station/VLAN/General VLAN Configuration" web page.

Transparent

In "Transparent" mode, the switch processes the incoming data packets as described in the "Frame Switching" section (see Section 3.3 on page 3-31). Neither the structure nor the contents of the data packets is changed. The information about VLAN assignment from a tag that may be contained in the data packet is ignored.

Tagging

In "Tagging" mode, incoming packets are received according to the specified VLAN rules, a VLAN tag is added, if required, and the packet is then processed by the switch and the management level according to the information in the tag. When transmitting Ethernet packets, the switch observes the rules for the relevant VLAN or the relevant output port.

The management VLAN ID specifies in which VLAN the switch can be accessed if it is operating in "Tagging" VLAN mode.

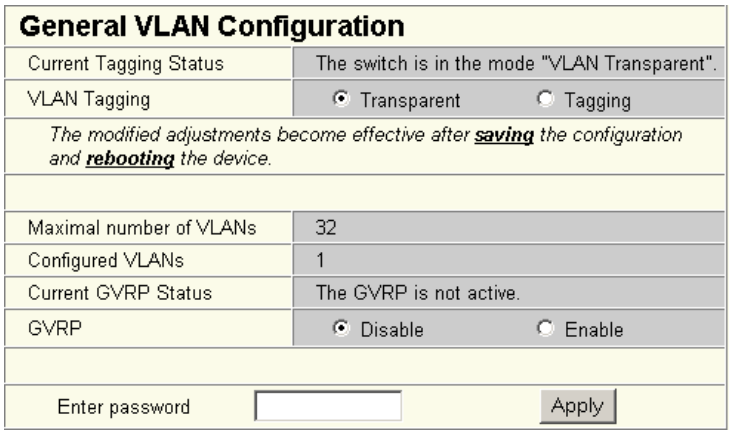


Figure 7-1 "General VLAN Configuration" menu

The switch supports a maximum of 32 different VLANs.

After switching the VLAN mode from "Tagging" to "Transparent" or vice versa, the active configuration must be saved and a device reset triggered so that the modification becomes active. The current valid state can be read in the "Current Tagging Status" line.

GVRP protocol

The GVRP protocol (GARP VLAN Registration Protocol) can be activated in **"VLAN Tagging" mode** for dynamic registration of the VLANs at the relevant neighbor. The GVRP switch indicates the selected user setting or enables the setting.

GVRP is used to dynamically create VLANs across several switches. If GVRP is set to "Disable", the switch is transparent for GVRP BPDUs (GVRP data packets).

If GVRP is active, the switch sends GVRP BPDUs every ten seconds. If the VLAN assignment of **a port** to a specified VLAN is changed, the adjacent switches will be informed of this change within the next 10 seconds.

When the GVRP is disabled, the adjacent switches also remove the dynamically learned ports within the next 10 seconds. If GVRP packets are missing, the learned group assignments are rejected after approximately 20 seconds.

If a static VLAN is installed on a switch, a port can be added to this VLAN via GVRP. The port is listed in the Current VLANs Table. However, only statically created group members are saved.

7.4 Current VLANs

The "Current VLANs" web page provides an overview of the VLANs currently created. In addition, refer to the table for the VLAN in which the switch is actually managed (see also ""IP Configuration" web page" on page 4-14). All static and dynamic VLANs are listed here. A distinction is made between tagged (T) and untagged (U) group members, as well as non-members (-) (see possible states on page 7-5).

Current VLANs

VID	Status	Group	Membership
1	static / Management Vlan	Ports 1-8	U U U U U U U U
		Ports 9-16	U U U U U U U U
12	static	Ports 1-8	- T T - - - - -
		Ports 9-16	- - - - - - - -
24	static	Ports 1-8	- - - - - - - -
		Ports 9-16	- - - - T U - -

(T=Tagged, U=Untagged, -=Non Member)

*This table, indicates, out of which ports, each VLAN's data is to be sent, using configuration data entered manually (i.e. web page **Static VLANs**) or entered automatically from **GVRP**.*

Note: This web page will be refreshed in 23 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces)!

Figure 7-2 "Current VLANs" web page

When the maximum number of created VLANs (static and/or dynamic) is reached, the following text appears below the key for the member states: "The switch supports only 32 VLANs! Further VLANs will be refused!"

VLAN 1 is always created statically and all ports are added to it as untagged members.

7.4.1 Static VLANs

Static VLANs can be created on this web page. Up to 31 new VLANs can be created (VLAN 2 to VLAN 32). If more are created, a corresponding message will be displayed.

VLAN 1 is always created statically and all ports are added to it as untagged members. By default upon delivery, with "Tagging" VLAN mode activated, network-based management interfaces (WBM, Telnet, and SNMP) are only available from VLAN 1. This means that in order to access the management interfaces, you must either implement data traffic in tagged mode without VLAN tag, where the switch is accessed via ports using the VLAN ID or you must use data traffic with VLAN tag, the ID of which is 1.

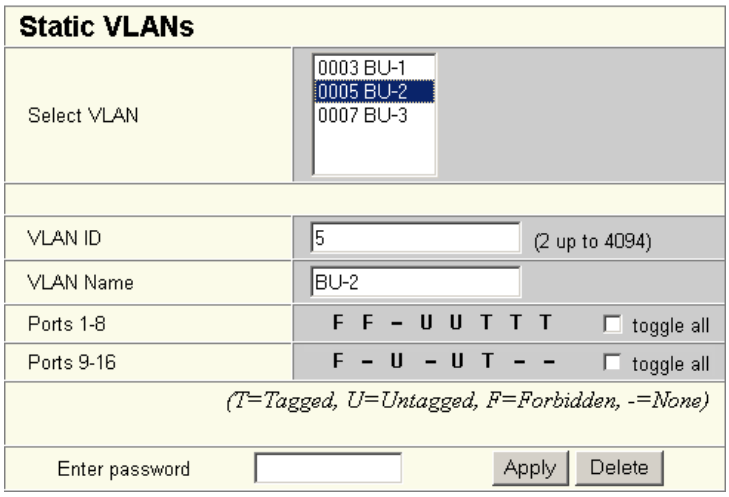


Figure 7-3 "Static VLANs" menu

On this web page you can create static VLANs by assigning a VLAN ID and VLAN name. The ports are then assigned to the individual VLANs by selecting the relevant VLAN and clicking on the character in the "Ports 1-8" line that indicates the current port status. Various options are selected by clicking on the status several times. By clicking on "toggle all", all available ports in the relevant port group change their status.

The possible states are:

T = Tagged

Ports with "Tagged" status belong to the selected VLAN and packets are sent to this port with VLAN tag.

U = Untagged

Ports with "Untagged" status belong to the selected VLAN and packets are sent to this port without VLAN tag. An "Untagged" port cannot belong to multiple VLANs - otherwise there is no logical division (except VLAN1).

F = Forbidden

Ports with "Forbidden" status do not belong to the selected VLAN and cannot be added dynamically to this VLAN via GVRP.

- **= None**

Ports with "None" status are not integrated into the VLAN.

7.4.2 VLAN Port Configuration

Port-specific VLAN settings can be made on this web page.

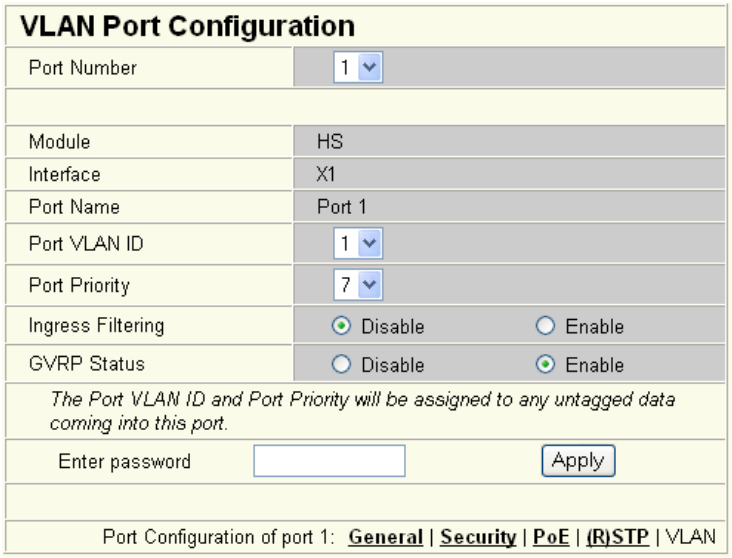


Figure 7-4 "VLAN Port Configuration" Menu

If "Ingress Filtering" is set to "Enable", the switch rejects data packets received at this port if is not a "tagged member" or "untagged member" of the VLAN with the VLAN ID contained in the tag of the packet.

Port Priority

– A corresponding tag indicating the priority is added to packets without tags.

Port VLAN ID

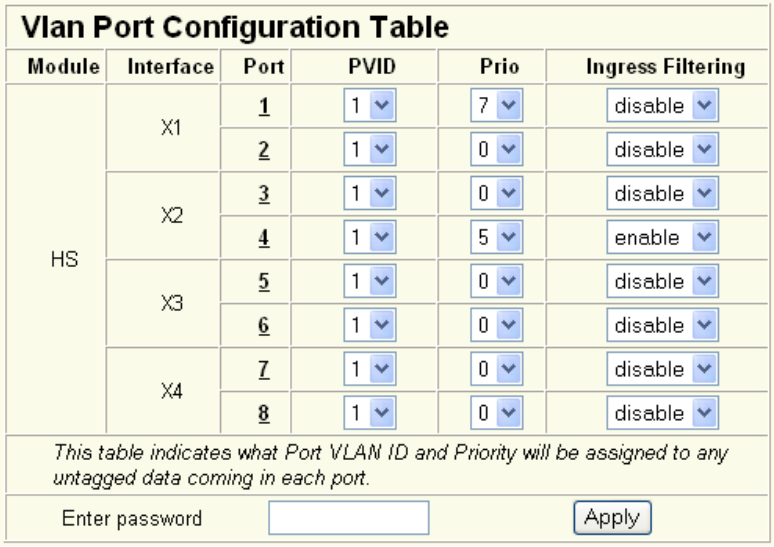
– Assignment of received, untagged packets to a VLAN. The corresponding VLAN ID must be set for the ports that are "untagged members" of a VLAN (see "Example: Communication between termination devices via VLAN" on page 7-8).

Only IDs of existing VLANs can be set as the port VLAN ID. If a VLAN is deleted, all port VLAN IDs that are set to this VLAN are reset to the default VLAN ID "1".

7.4.3 VLAN Port Configuration Table

This web page provides an overview of the main VLAN settings for the ports. Clicking on the relevant port number opens the "VLAN Port Configuration" web page, where the settings can be modified.

This table can be used to assign incoming packets to the created VLANs if the packets reached the port without VLAN tag.



Vlan Port Configuration Table

Module	Interface	Port	PVID	Prio	Ingress Filtering
HS	X1	1	1	7	disable
		2	1	0	disable
	X2	3	1	0	disable
		4	1	5	enable
	X3	5	1	0	disable
		6	1	0	disable
	X4	7	1	0	disable
		8	1	0	disable

This table indicates what Port VLAN ID and Priority will be assigned to any untagged data coming in each port.

Enter password [ ] Apply

Figure 7-5 "VLAN Port Configuration Table" menu

7.5 Creating Static VLANs

Security recommendation: Instead of using VLAN 1 for management, it is recommended that a new separate VLAN is created for management. Make sure that the administrator has access to this VLAN.

Warnings displayed when creating/configuring VLANs indicate configuration errors:

– An "untagged" port belongs to **multiple** VLANs.
– The port assignment (untagged) and PVID **do not** match.

In order to create a VLAN, the switches involved must be configured accordingly. In the following example, data traffic is to be enabled in VLAN 5 between termination devices A and B.

The type of termination device must be taken into consideration: VLAN-compatible (processes tags) or not VLAN-compatible (does not process tags). In the example, two types of termination device are take into consideration.

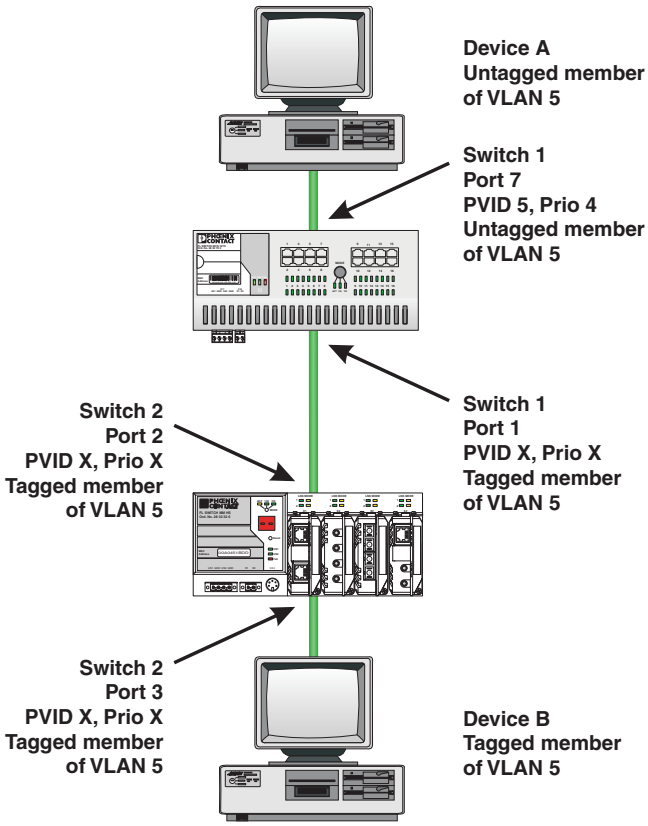


Figure 7-6 Example: Communication between termination devices via VLAN

Switch Configuration

1. Set both switches to "VLAN Tagging" mode, save, and restart devices.
2. Create VLAN 5 on switch 1 and specify port 7 as an "untagged" member and port 1 as a "tagged" member.
3. For port 7 at switch 1, set the port VLAN ID to 5 and the port priority to any.
4. On switch 2, create port 2 and port 3 as "tagged" members of VLAN 5.

Both termination devices now communicate via the network path shown in the example without other switch ports forwarding the broadcast packets for both termination devices, for example.

If additional infrastructure components are located between switch 1 and switch 2, there are two options to ensure communication between the termination devices:

1 The infrastructure is also operated in "VLAN Tagging" mode and VLAN 5 is created based on the relevant devices. Result: high configuration and maintenance costs.
2 GVRP is activated in "VLAN Tagging" mode on all infrastructure components and the information about the created VLANs is transmitted within the network via switch 1 and switch 2. Result: bidirectional data exchange is ensured between termination device A and B.

7.5.1 Dynamic Configuration

Dynamic VLAN configuration using GVRP can be set for transmission between infrastructure components. Here, every switch with static or dynamically created VLANs transmits information within the network via VLAN IDs. The adjacent switches with activated GVRP then create the same VLANs and add the receiver ports of the GVRP BPDUs as "tagged" ports. A BPDU receiver then distributes its own BPDUs to all ports via the dynamically learned VLAN.

Switch Configuration

1 All switches must be set to "VLAN Tagging" mode. After saving the configuration, a restart is required.
2 GVRP must be activated on all switches.

Since termination devices usually do not support VLAN tags, port-specific settings must be made at the termination device ports for the infrastructure. The switch then adds the corresponding tags to every data packet received at the relevant port. If a data packet is to be sent from the termination device port to the termination device, the switch removes the VLAN tag first.

7.6 VLAN and (R)STP

When using (R)STP and VLAN simultaneously, please note the following:
– (R)STP is **not** based on VLANs
– (R)STP creates a loop-free topology in the form of a tree structure

In the event of static VLAN configuration, all possible redundant data paths must be taken into consideration in the configuration. All possible backbone ports of the network (not the termination device ports) must be inserted in all available VLANs as "tagged" members. This ensures that for every possible tree structure that can be generated by (R)STP, every VLAN can be accessed by every switch.

A typical configuration is illustrated in the following diagram:

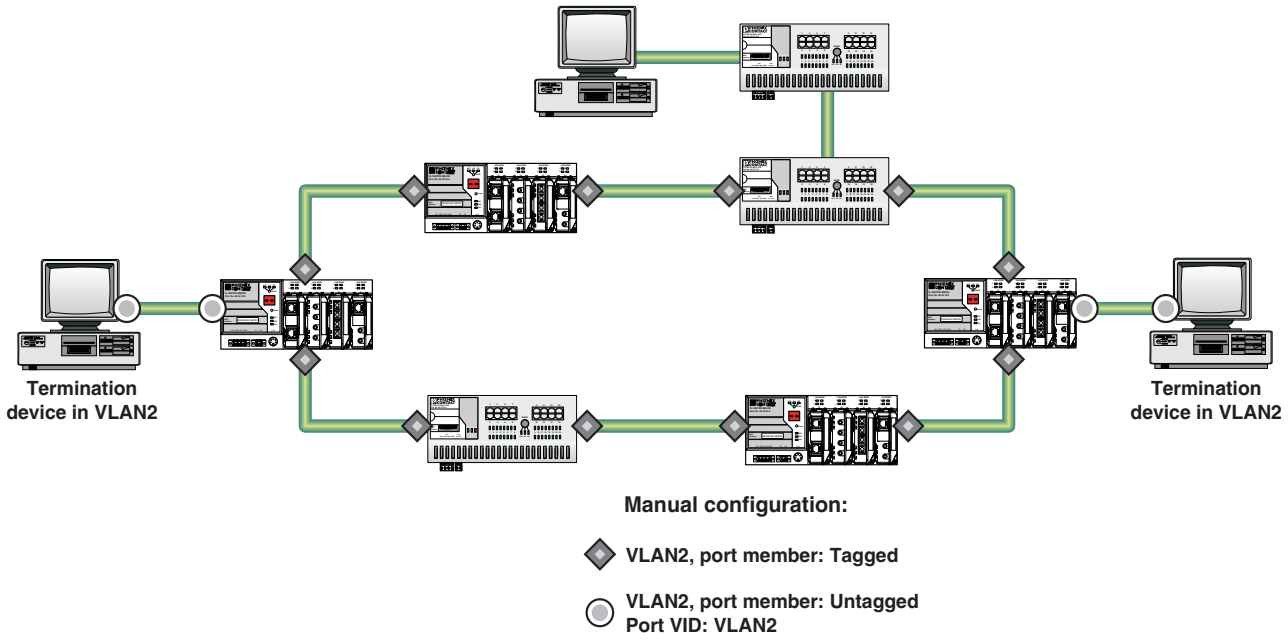


Figure 7-7 Typical configuration for VLAN and (R)STP

8 Operating as a PROFINET Device

The switch is supported as a PROFINET device in PC WorX Version 5.00.26 or later. In a PROFINET application, the PROFINET IO controller is responsible for starting up the switch. This includes assigning the IP parameters, comparing the desired/actual configuration, and archiving alarms sent by the switch. In the event that a device is replaced, the control system detects the replacement device and starts it up automatically. For the control program, the switch as a PROFINET IO device provides the link states as a process data item.

8.1 Preparing the Switch for PROFINET Mode

By default upon delivery the switch operates in "Default" mode and must be set to "PROFINET" mode once.

Switching to "PROFINET" mode

Two mechanisms are available for switching the mode:

– Following startup and assignment of an IP address, the operating mode can be changed on the corresponding page in WBM (see ""Operating Mode" Web Page"on page 4-20)
– Through configuration via the serial interface (see "Management via Local V.24 (RS-232) Communication Interface"on page 4-116)

When activating "PROFINET" mode, the following default settings are made for operation:

– The Link Layer Discovery Protocol (LLDP) is enabled with the following configuration specifications for PROFINET components:
  - Message transmit interval: 5 s
  - Message transmit hold multiplier: 2
  - TLV port ID with subtype locally assigned in the following format: port-xyz
  - TLV chassis ID with subtype locally assigned transmits the station name
– The Discovery and Configuration Protocol (DCP) is activated as the mechanism for assigning IP parameters.
– The station name (system name) is deleted if the value for the "System Name" object contains the device type (default upon delivery).

In addition, when switching to "PROFINET" mode, the configuration is saved automatically and the device is restarted.

The switch then starts in "PROFINET" mode for the first time and waits for a PROFINET IP address to be assigned. At this point, the switch is already visible in the network via LLDP with the default name "FL SWITCH MM HS" and the IP address "0.0.0.0".

Waiting for a valid IP configuration via DCP is indicated by the switch with "dP" in the display and by the flashing of the LED for the currently active mode.

The switch cannot be accessed via other network services such as ping at this time.

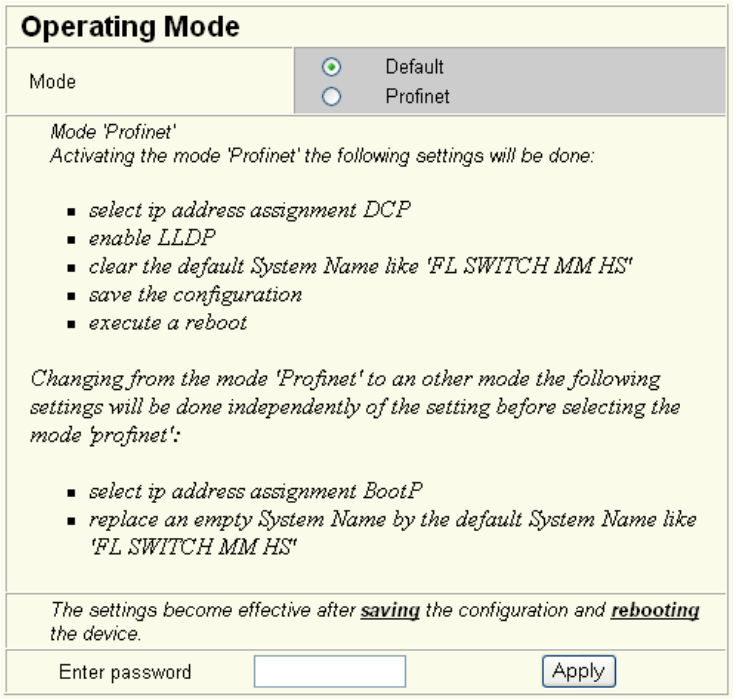

Operating Mode
Mode
Default
Profinet
Mode 'Profinet'
Activating the mode 'Profinet' the following settings will be done:
select ip address assignment DCP
enable LLDP
clear the default System Name like 'FL SWITCH MM HS'
save the configuration
execute a reboot
Changing from the mode 'Profinet' to an other mode the following settings will be done independently of the setting before selecting the mode 'profinet':
select ip address assignment BootP
replace an empty System Name by the default System Name like 'FL SWITCH MM HS'
The settings become effective after saving the configuration and rebooting the device.
Enter password
Apply

Figure 8-1 "Operating Mode" web page

Switching to "Default" mode

When the switch is reset to "Default" mode from "PROFINET" mode, the following settings are made:

– LLDP remains active with the values default upon delivery.
– IP address assignment is set to BootP.
– The station name for the switch does not change. If no station name has been specified, the device type is entered.

It is recommended to save the new configuration after changing operating mode. Please note that some configuration modifications only take effect after a restart.

8.2 Switch as a PROFINET IO Device

8.2.1 Configuration in the Engineering Tool

8.2.1.1 Specifying the Bus Configuration

The switch can be operated as a PROFINET IO device if it is integrated under a control system in the bus configuration in the engineering tool.

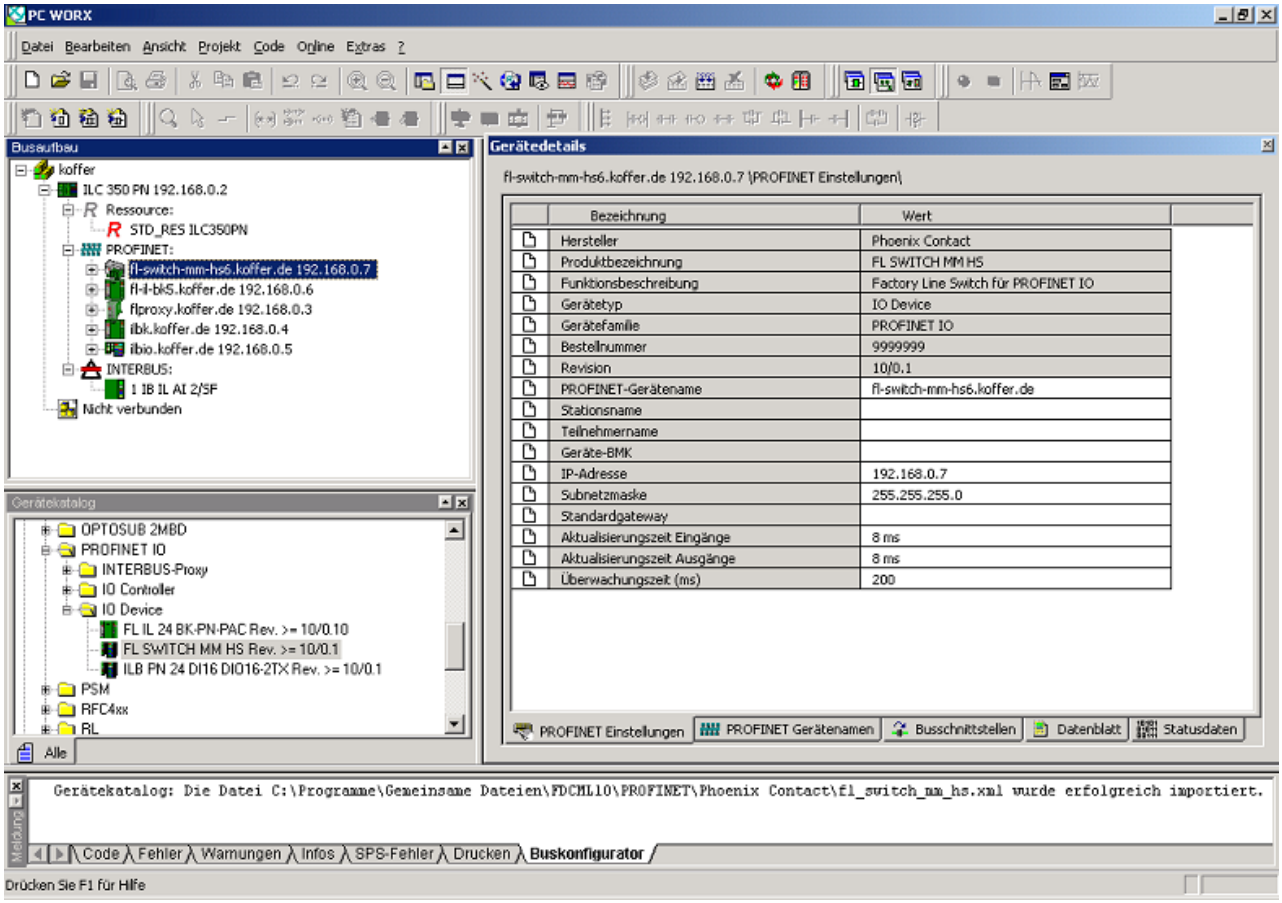


Figure 8-2 The switch in the bus configuration under PC WorX

If the switch is not listed in the device catalog, the device description provided by Phoenix Contact must be imported. The latest device description can be downloaded at www.download.phoenixcontact.com.

If the device description is available in the device catalog, the following options are available for bus configuration:

– Manual - The components are transferred to the bus configuration from the device catalog using drag & drop.
– Automatic - The devices are entered via the "Read PROFINET" function, which means that they can be accessed in the network via DCP (Discovery and Configuration Protocol). For this, the devices must be supplied with power and the operating mode must be set to "PROFINET".

Interface Modules and Bus Configuration

– No interface modules configured -> IP address assignment only by the control system
– All interface modules configured correctly -> IP address assignment by the control system, transmission of process data and alarms from configured slots

– One or more interface modules configured incorrectly -> Following startup, the MMS indicates "Cd" (configuration difference) in the display

If "Cd" appears in the display, insert the correct interface modules and restart the switch.

The desired/actual configuration is no longer monitored during the system runtime.

8.2.2 Configuring the Switch as a PROFINET IO Device

Once all switches have been added to the bus configuration, the following settings must be made for the individual switches via the "Detail View" tab (device details):

– The PROFINET device name must be checked and modified, if necessary.
– The IP address and the subnet mask must be checked and modified, if necessary.
– The update time for inputs should be set to **"512 ms"** (default).
– The update time for outputs should be set to **"512 ms"** (default).
– The monitoring time should be set to **"2000 ms"** (default).
– The interface modules must be selected from the module catalog and added to the station.

Gerätedetails

FL SWITCH MM HS pn-mms61 172.16.27.61 \PROFINET Einstellungen\

Bezeichnung	Wert	
Hersteller	Phoenix Contact	
Produktbezeichnung	FL SWITCH MM HS	
Funktionsbeschreibung	Modularer managbarer Switch als Profinet IO D...	
Gerätetyp	Switch	
Gerätefamilie	FL	
Bestellnummer	2832328	**Set by the user:**
Revision	00 / 4.00	
DNS/PROFINET-Gerätename	fl-switch-mm-hs6.koffer.de	← **Station name**
Stationsname		
Teilnehmername		
Geräte-BMK		
IP-Adresse	172.16.27.61	← **IP address**
Subnetzmaske	255.255.0.0	← **Subnet mask**
Standardgateway		
Aktualisierungszeit Eingänge	512 ms	← **Recommended value**
Aktualisierungszeit Ausgänge	512 ms	← **Recommended value**
Überwachungszeit (ms)	2000	← **Recommended value**
Betrieb bei Konfigurationsunterschieden	nein	
Oberster Knoten in Ethernet-Topologie	nein	
Verbindungszustand protokollieren	ja	

Figure 8-3 Device details with modified settings

The PROFINET variables can then be created and used in the control program.

In addition to the "PNIO_DATA_STATE" standard variables, the switch provides the link status as a process data byte for each port. If the "PNIO_DATA_VALID" bit for the "PNIO_DATA_STATE" variables declares the switch process data as valid, the process data item for a port can have the following values:

– Value = 1 - active link
– Value = 2 - no active link
– Value = 3 - link present, but partner cannot establish link (only for FX ports - Far End Fault Detection)

Process data can only be accessed if the parameterized desired configuration on device startup corresponds to the actual configuration.

The "Status" word and the "Control" word of the management agent are not used.

8.2.3 PROFINET Flashing Function

If the switch is requested to flash in PROFINET mode by the engineering tool, "00" and the previous current indication alternately flash in the display.

8.2.4 Naming the Device

In order to start up a switch in "PROFINET" mode, each switch must be assigned a name once, i.e., each PROFINET device is assigned a unique device name. A device search ("Read PROFINET" function in PC WorX) is performed via the engineering tool, where all the devices that can be accessed in the network are listed. After identifying unknown devices via the specified MAC address or the "flashing" function, the device name configured in the engineering tool is saved permanently on the switch with the "Assign Name" function.

The device name can also be assigned via WBM before switching to "PROFINET" mode.

8.2.5 Operating in the PROFINET Environment

A switch that has already been assigned a name starts in "PROFINET" mode without an IP address and waits for the assignment of an IP configuration ("dP" in the display and flashing of the LED for the currently active mode). Once the project has been translated and downloaded to the control system, the control system implements startup and configuration. As soon as a communication relationship has been successfully established between the switch and the control system, the switch starts its management interface. The switch indicates that the PROFINET connection has been established correctly by an entry in the results table and the appearance of an additional dot in the bottom-right corner of the display.

If the MMS has established a PROFINET connection, a dot appears in the bottom-right corner of the display.

8.3 PROFINET Alarms

8.3.1 Alarms in WBM

In "PROFINET" mode, the "PROFINET Alarms" web page appears in the navigation bar under "Switch Station/Diagnostics". Here, all alarms supported by the IO device can be activated. The PROFINET alarms are sent to the control system by the IO devices. From there they can be read from the diagnostics archive using "DIAG+" (Version 2.0 is included in Service Pack 1 for PC WorX 5.00.26).

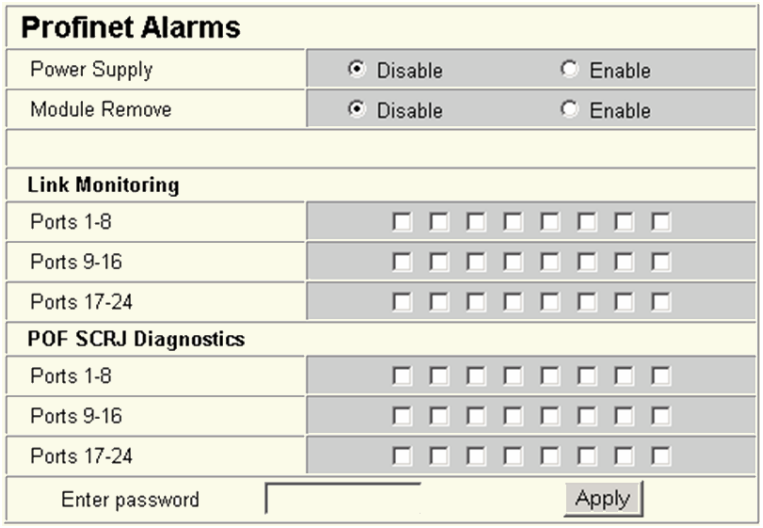


Figure 8-4 PROFINET alarms in WBM

9 LLDP (Link Layer Discovery Protocol)

9.1 Basics

LLDP

The switch supports LLDP according to IEEE 802.1ab and enables topology detection of devices that also have LLDP activated.

Advantages of using LLDP:

– Improved error location detection.
– Improved device replacement.
– More efficient network configuration.

The following information is received by neighbors or sent to neighbors, as long as LLDP is activated:

– The device sends its own management and connection information to neighboring devices.
– The device receives management and connection information from neighboring devices.

Displaying LLDP information

The information that is collected is presented in a table in WBM. The table includes port numbers that are used to connect both devices together, as well as the IP address, the device name of neighboring devices, and the device type.

LLDP general

The Link Layer Discovery Protocol (LLDP) according to 802.1ab is used by network devices to learn and maintain the individual neighbor relationships.

Function

A network infrastructure component transmits a port-specific BPDU (Bridge Protocol Data Unit) at the "Message Transmit Interval", which contains the individual device information, to each port in order to distribute topology information. The partner connected to the relevant port learns the corresponding port-specific neighbors from these BPDUs.

The information learned from the BPDUs is saved for a defined period of time as the TTL value (TTL - Time To Live). Subsequent receipt of the same BPDUs increases the TTL value again and the information is still saved. If the TTL elapses, the neighbor information is deleted.

An MMS manages a maximum of 50 items of neighbor information, all other information is ignored.

If several neighbors are displayed on one switch port, then there must be at least **another** switch/hub installed **between** this switch and the neighbor indicated, which LLDP does not support or has not activated.

Table 9-1 Event table for LLDP

Event	Activity of the Individual LLDP Agent	Response of the Neighboring LLDP Agent
Activate LLDP agent or device startup	Transmit LLDP BPDUs to all ports	Include sender in the list of neighbors
Deactivate LLDP agent or software reset	Transmit LLDP BPDUs with a TTL value of 0 seconds to all ports	Delete sender from the list of neighbors
Link up	Send port-specific LLDP BPDUs	Include sender in the list of neighbors
Link down	Delete all neighbors for this port	-
Timer (Message Transmit Interval)	Cyclic transmission of BPDUs to all ports	Update information
Aging (Time To Live)	Delete neighbor information	-
Receiving a BPDU from a new neighbor	Extend list of neighbors and respond with port-specific BPDU	Include sender in the list of neighbors

Link Layer Discovery Protocol

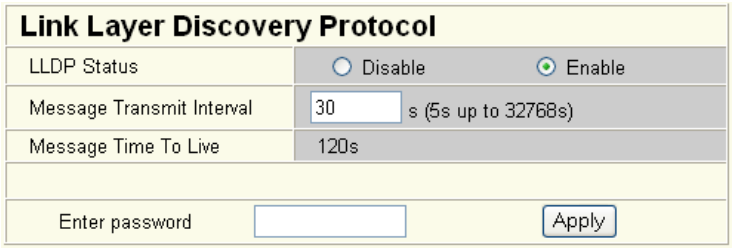


Figure 9-1 "Link Layer Discovery Protocol" web page

The "Message Time To Live" is determined by multiplying the "Message Transmit Interval" with the "Message Transmit Hold Multiplier". The "Message Transmit Hold Multiplier" can only be modified via SNMP. The default value is four.

LLDP Topology

LLDP Topology

Local	Neighbors			
Port	Type	Address	Device	Port
1		192.168.0.45	FL SWITCH MM HS	7
12		192.168.0.3	fl-il-bk2.quicks...	port-001
11		192.168.0.5	fl-pn-ibs4.quick...	port-001

Note: This web page will be refreshed in 26 sec automatically (change the interval at the web page 'Device Configuration / User Interfaces')!

Figure 9-2 "LLDP Topology" web page

A table is created for known neighbors and contains the following five columns:

– Local Port
  Contains the port number of the local switch that is used to connect a neighbor to this switch. The port number is also a link to the local "Port Configuration" web page.
– Type
  An icon is displayed here, which corresponds to the neighboring device type. "Ethernet Device" is displayed in general for devices produced by other manufacturers.
– Address
  Indicates the management IP address for the neighbor.
– Device
  Indicates the system name of the neighbor.
– Indicates the port number of the neighboring switch that is used to connect the neighbor to the local switch. If the neighbor is identified as a Phoenix Contact switch, the port number is implemented as a link to the "Port Configuration" web page for the neighbor.

9.2 Representation of the Topology in an Engineering Tool

The LLDP information can be represented as such or similarly in engineering tools.

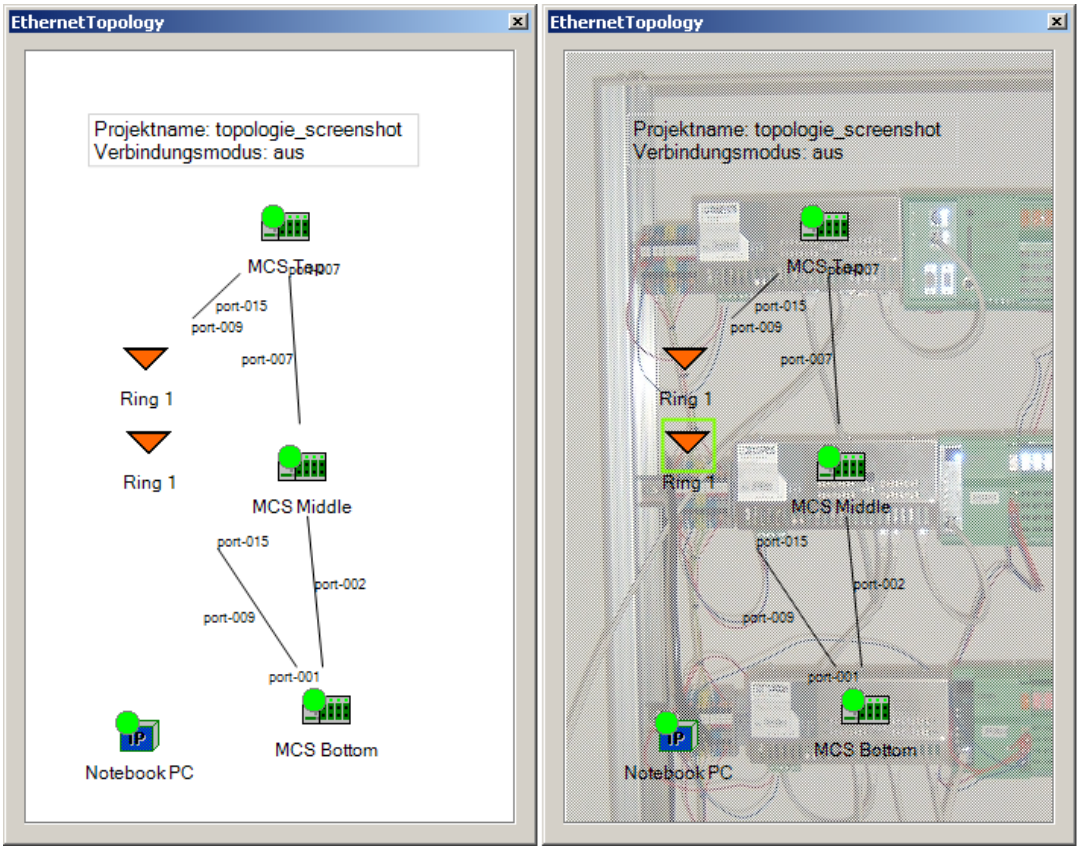


Figure 9-3 Representation of the topology

10 DHCP Relay Agent

The MMS is able to act as a DHCP relay agent. The DHCP relay agent function is required for DHCP option 82. DHCP option 82 is used by the DHCP server when assigning addresses to identify the requesting termination device via the corresponding physical switch port. In the event of device replacement, DHCP option 82 enables the replacement device to be assigned the same IP address as the replaced device due to the physical position in the network. The DHCP packet (broadcast) originally sent by the termination device also reaches the DHCP server if it is located in the same subnetwork. The DHCP server should be set so that it ignores this packet.

Sequence:

Every time the MMS receives a DHCP discover/request that has been sent by a termination device, the MMS extends the "DHCP option 82" field and forwards the data packet to the specific DHCP server. The desired DHCP server should be configured in WBM on the "Relay Agent" page.

The DHCP server can generate a response using option 82 information and can send this to the relay agent.

The switch then removes the DHCP option 82 data from the DHCP server response and forwards it to the termination device that triggered the request.

Information in the DHCP option 82 field:

The MMS extends the VLAN ID in the DHCP option 82 field for the VLAN to which the termination device is assigned and the switch port to which the termination device is connected. In addition, the MMS enters its own DHCP option 82 remote ID in the field. The DHCP option 82 remote ID can be configured by the user and contains the IP or MAC address of the MMS.

10.1 Activating the DHCP Relay Agent

Enable the web page via "General Configuration/User Interfaces". Activate the agent with "Enable", specify at least the IP address of the server.

The MMS management does not start the relay agent while the switch is operating as a DHCP client.

10.1.0.1 Disabling the Relay Agent According to the Port

In firmware Version 4.50 or later, the DHCP relay agent function can be disabled according to the port. No DHCP option 82 packets are sent by the deactivated ports.

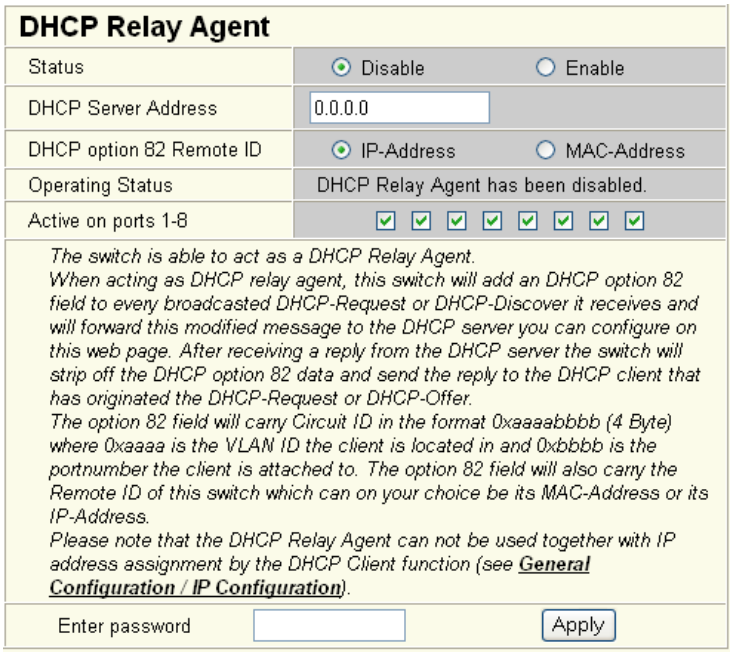

DHCP Relay Agent
Status
Disable
Enable
DHCP Server Address
0.0.0.0
DHCP option 82 Remote ID
IP-Address
MAC-Address
Operating Status
DHCP Relay Agent has been disabled.
Active on ports 1-8
The switch is able to act as a DHCP Relay Agent.
When acting as DHCP relay agent, this switch will add an DHCP option 82 field to every broadcasted DHCP-Request or DHCP-Discover it receives and will forward this modified message to the DHCP server you can configure on this web page. After receiving a reply from the DHCP server the switch will strip off the DHCP option 82 data and send the reply to the DHCP client that has originated the DHCP-Request or DHCP-Offer.
The option 82 field will carry Circuit ID in the format 0xaaaabbbb (4 Byte) where 0xaaaa is the VLAN ID the client is located in and 0xbbbb is the portnumber the client is attached to. The option 82 field will also carry the Remote ID of this switch which can on your choice be its MAC-Address or its IP-Address.
Please note that the DHCP Relay Agent can not be used together with IP address assignment by the DHCP Client function (see General Configuration / IP Configuration).
Enter password
Apply

Figure 10-1 "Relay Agent" web page

The "DHCP Relay Agent" function and IP address assignment via DHCP cannot be activated at the same time.

11 Technical Data and Ordering Data

11.1 Technical Data

General Data	
Function	Modular Managed Ethernet/Fast Ethernet Switch; conforms to standard IEEE 802.3
Switch principle	Store-and-forward
Address table	8000 MAC addresses
SNMP	Version 1 and 2c
Transmission capacity per port 64-byte packet size, half duplex	At 10 Mbps: 14,880 pps (packets per second) At 100 Mbps: 148,800 pps
Supported MIBs	MIB II, RMON MIB, bridge MIB, If MIB, Etherlike MIB, and Phoenix Contact private SNMP objects
Housing dimensions (width x height x depth) in mm	
Head station	214 x 95 x 107 (depth from top edge of DIN rail)
Head station with one extension module	341 x 95 x 107 (depth from top edge of DIN rail)
Head station with two extension modules	468 x 95 x 107 (depth from top edge of DIN rail)
Permissible operating temperature	0°C to +55°C
Permissible storage temperature	-20°C to +70°C
Degree of protection	IP20, DIN 40050, IEC 60529
Protection class	Class 3 VDE 0106; IEC 60536
Laser protection - fiber optic interface modules	Class 1 according to EN 60825-1
Humidity	
Operation	10% to 95%, no condensation
Storage	10% to 95%, no condensation
Air pressure	
Operation	80 kPa to 108 kPa, 2000 m above sea level
Storage	70 kPa to 108 kPa, 3000 m above sea level
Mounting position	Perpendicular to a standard DIN rail
Connection to protective earth ground	Snapped onto a grounded DIN rail
Weight of head station	1350 g, typical

Supply Voltage (US1/US2 Redundant)	
Connection	Via COMBICON; conductor cross section = 2.5 mm^2, maximum
Nominal value	24 V DC (SELV)
Permissible voltage range	18.0 V DC to 32.0 V DC
Test voltage	500 V DC for one minute
Typical current consumption on US at 24 V DC	0.35 ... 3.25 A, depending on configuration (extensions/interface modules)
Typical power consumption	8.4 W ... 78 W, depending on configuration (extensions/interface modules); see example on page 11-5

Interfaces at the Head Station	
Number of slots for interface modules	4
Connection medium	Via interface modules, flexible media support
Number of Ethernet ports	
Head station	8
Head station and one extension module	16
Head station and two extension modules	24
System interface for extension module	
Number of extension modules	2
Transmitted signals	Supply voltage, control signals, data
V.24 (RS-232) communication interface	
Connection format	Mini-DIN female connector
Floating alarm contact	
Voltage	24 V DC
Current carrying capacity	100 mA, maximum

Interfaces at the Extension Modules	
Number of slots for interface modules	4
Connection medium	Via interface modules, flexible media support
Number of Ethernet ports	8
System interface for extension module	Incoming and outgoing system bus interface
Transmitted signals	Supply voltage, control signals, data

RJ45 Interfaces (Standard)	
Number	2
Connection format	8-pos. RJ45 female connector on the switch
Connection medium	Twisted pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 Ohm
Transmission speed	10/100 Mbps
Maximum network segment expansion	100 m

RJ45 Interfaces – Power over Ethernet IEEE 802.3af	
Number	2
Connection format	8-pos. RJ45 female connector on the switch
Connection medium	Twisted pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 Ohm
Transmission speed	10/100 Mbps
Maximum network segment expansion	100 m
Complete configuration support	Firmware Version 4.0 or later, system bus firmware 5.00 or later in the head station, and system bus firmware 4.00 or later in the extension modules
Connection of the PoE supply	Via COMBICON; conductor cross section = 2.5 mm^2, maximum
Nominal value	48 V DC (SELV)
Permissible voltage ranges	44 V DC to 53 V DC

RJ45 Interfaces – Power over Ethernet IEEE 802.3af (Continued)	
Test voltage	500 V AC for one minute
Maximum current consumption on US at 48 V DC	900 mA
Typical power consumption	40 W

Ethernet Interface (SC) – Multi-Mode	
Number	2
Connection format	SC duplex female connector on the switch
Wavelength	1300 nm
Laser protection	Class 1 according to DIN EN 60825-1:2001-11
Minimum transmission length including 3 dB system reserve	6.4 km glass fiber with F-G 50/125 0.7 dB/km F1200 2.8 km glass fiber with F-G 50/125 1.6 dB/km F800 10 km glass fiber with F-G 62.5/125 0.7 dB/km F1000 3.0 km glass fiber with F-G 62.5/125 2.6 dB/km F1000
(Average) dynamic transmission power (fiber type) in link mode	
Minimum	-23.5 dBm (50/125 µm)/-20 dBm (62.5/125 µm)
Maximum	-14 dBm (50/125 µm)/-14 dBm (62.5/125 µm)
Static transmission power (fiber type)	
Minimum	-20.5 dBm (50/125 µm)/-17 dBm (62.5/125 µm)
Maximum	-11 dBm (50/125 µm)/-11 dBm (62.5/125 µm)
Minimum receiver sensitivity	-31 dBm (dynamic)/-28 dBm (static)
Maximum overrange	-14 dBm (dynamic)/-11 dBm (static)
Transmission speed	100 Mbps

Ethernet Interface (SC) – Single Mode	
Number	2
Connection format	SC duplex female connector on the switch
Wavelength	1300 nm
Laser protection	Class 1 according to DIN EN 60825-1:2001-11
Minimum transmission length including 3 dB system reserve	36 km glass fiber with F-G 9/125 0.36 dB/km 32 km glass fiber with F-G 9/125 0.4 dB/km 26 km glass fiber with F-G 9/125 0.5 dB/km
(Average) dynamic transmission power (fiber type) in link mode	
Minimum	-15.0 dBm (9/125 µm)
Maximum	-8.0 dBm (9/125 µm)
Minimum receiver sensitivity	> -31 dBm (9/125 µm)
Maximum overrange	> -7 dBm (9/125 µm)
Transmission speed	100 Mbps

Ethernet Interfaces – POF-SMA	
Number	1 (FL IF TX/POF 100...) 2 (FL IF 2POF 100...)
Connection format	F-SMA female connectors on the interface module
Data transmission rate	10/100 Mbps
Wavelength	650 nm
Minimum cable length	1 m
Transmission length including 3 dB system reserve	50 m polymer fiber with F-K 980/1000 230 dB/km

Ethernet Interfaces – POF-SMA (Continued)	
(Average) dynamic transmission power (fiber type) in link mode	
Minimum	-8.0 dBm (980/1000 µm) Reduced by -12 dBm (980/1000 µm) via switch
(Average) dynamic receiver sensitivity (fiber type) in link mode	
Minimum	-23.0 dBm (980/1000 µm)
Optical overrange	-11.5 dBm (980/1000 µm)

Ethernet Interfaces – HCS	
Number	2
Connection format	F-SMA female connectors on the interface module
Data transmission rate	100 Mbps
Wavelength	650 nm
Transmission length including 3 dB system reserve	100 m HCS fiber with F-S 200/230 10 dB/km
(Average) dynamic transmission power (fiber type) in link mode	
Minimum	-13 dBm (200/230 µm)
(Average) dynamic receiver sensitivity (fiber type) in link mode	
Minimum	-23.0 dBm (200/230 µm)
Optical overrange	-11.5 dBm (200/230 µm)

Ethernet Interfaces – SCRJ With Optical Diagnostics	
Number	2 (FL IF 2POF SCRJ-D)
Connection format	SC-RJ female connectors on the interface module
Data transmission rate	10/100 Mbps (100 Mbps according to PROFINET standard)
Wavelength	660 nm
Laser protection	Class 1 according to DIN EN 60825-1
Minimum cable length	1 m
Transmission length including 3 dB system reserve	50 m polymer fiber with F-K 980/1000 230 dB/km at 10/100 Mbps, maximum 100 m HCS fiber with F-S 200/230 8 dB/km at 100 Mbps, maximum
(Average) dynamic transmission power (fiber type) in link mode	
Minimum	-8.0 dBm (980/1000 µm)
(Average) dynamic receiver sensitivity (fiber type) in link mode	
Minimum	-23.0 dBm (980/1000 µm)
Optical overrange	1.0 dBm (980/1000 µm)

Cable Lengths	
Twisted pair	100 m
Polymer fiber (POF)	Depends on the interface module 1 m, minimum
HCS	Depends on the interface module
Glass fiber 1300 nm (multi-mode)	6400 m with glass fiber with F-G 50/125 0.7 dB/km F1200 2800 m with glass fiber with F-G 50/125 1.6 dB/km F800 10,000 m with glass fiber with F-G 62.5/125 0.7 dB/km F1000 3000 m with glass fiber with F-G 62.5/125 2.6 dB/km F600
Glass fiber 1300 nm (single mode)	36,000 m with glass fiber with F-G 9/125 0.36 dB/km 32,000 m with glass fiber with F-G 9/125 0.4 dB/km 26,000 m with glass fiber with F-G 9/125 0.5 dB/km

Mechanical Tests	
Shock test according to IEC 60068-2-27	Operation: 25g, 11 ms period, half-sine shock pulse Storage/transport: 50g, 11 ms period, half-sine shock pulse
Vibration resistance according to IEC 60068-2-6	Operation/storage/transport: 5g, 10 - 150 Hz, Criterion 3
Free fall according to IEC 60068-2-32	1 m

Conformance With EMC Directives	
Noise emission according to EN 55011	Class A
Warning: The limit values of the electromagnetic noise emission according to EN 55011, Class A are only observed by the module if it is installed in a grounded metal control cabinet.	
Radio interference field strengths according to EN 55022	Class A
Electrostatic discharge (ESD) according to EN 61000-4-2	Class 3; Criterion B
Electromagnetic fields according to IEC 61000-4-3	10 V/m; Criterion A
Conducted interference according to IEC 61000-4-6	10 V_{RMS}; Criterion A
Fast transients (burst) according to IEC 61000-4-4	Data lines: 1 kV; Criterion A Power supply lines: 2.2 kV; Criterion B
Surge voltages according to IEC 61000-4-5	Data lines: ±1 kV asymmetrical; Criterion B Power supply lines: ±0.5 kV symmetrical/asymmetrical; Criterion B

Differences Between This Version and Previous Versions
Version 01: "Spanning Tree" section added; FL IF 2FX SM ... added
Version 02: Technical data for POF interface added
Version 03: Multicast filtering added, data for interface modules revised
Version 04: Extended multicast filtering added, improved handling described for the memory module
Version 05: VLAN and RSTP added, as well as new interface modules and GL certification
Version 06: Supplement for Environmental Category 1 added
Version 07/8: Functions and new features of firmware Version 4.0 and interface modules extended
Version 09: Functions and new features of firmware Version 4.50, interface modules and accessories extended

11.2 Typical MMS Current Consumption (Example)

Typical Module Current Consumption	
FL SWITCH MM HS [1]	350 mA
FL MXT [2]	250 mA
FL IF 2TX VS-RJ ... [3]	0 mA
FL IF 2HCS 100 ... [4]	100 mA
FL IF 2FX (SM) SC or ST ... [5]	200 mA
FL IF TX/POF 10/100 ... [6]	60 mA
FL IF TX/HCS 100 ... [7]	60 mA
FL IF MEM ... [8]	0 mA
FL IF 2PSE ...	30 mA (from MMS, additional 850 mA, maximum from external 48 V PoE supply)
FL IF 2POF SCRJ-D	200 mA

Typical Module Current Consumption (Continued)
Example Structures
Station with 2 FX modules and 2 TX modules 350 mA [1] + (2 x 200 mA [5]) + (2 x 0 mA [3]) = 750 mA
Station with 2 FX modules, 5 HCS modules, and 1 POF/TX module 350 mA [1] + 250 mA [2] + (2 x 200 mA [5]) + (5 x 100 mA [4]) + 60 mA [6] = 1560 mA
Station with 5 FX modules, 4 HCS modules, 2 TX modules, and 1 POF/TX module 350 mA [1] + (2 x 250 mA [2]) + (5 x 200 mA [5]) + (4 x 100 mA [4]) + (2 x 0 mA [3]) + 60 mA [6] = 2310 mA

11.3 Ordering Data

Products

Description	Order Designation	Order No.	Pcs./Pck.
Modular Managed Switch - head station	FL SWITCH MM HS	2832328	1
Extension module with four slots for eight ports	FL MXT	2832331	1
Configuration cable for connecting the switch with a PC, V.24 (RS-232)	PRG CAB MINI DIN	2730611	1
Universal end clamp	E/NS 35 N	080088 6	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format for connection on the **front**	FL IF 2TX VS-RJ-F	2832344	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format for connection on the **bottom**	FL IF 2TX VS-RJ-D	2832357	1
Interface module with 2 × glass fiber (multi-mode) 100 Mbps in SC format for connection on the **front**	FL IF 2FX SC-F	2832412	1
Interface module with 2 × glass fiber (multi-mode) 100 Mbps in SC format for connection on the **bottom**	FL IF 2FX SC-D	2832425	1
Interface module with 2 × glass fiber (multi-mode) 100 Mbps in B-FOC (ST®) format for connection on the **bottom**	FL IF 2FX ST-D	2884033	1
Interface module with 2 × glass fiber (single mode) 100 Mbps in SC format for connection on the **front**	FL IF 2FX SM SC-D-F	2832205	1
Interface module with 1 × twisted pair 10/100 Mbps in RJ45 format and 1 × polymer fiber 10/100 Mbps in F-SMA format for connection on the **bottom**	FL IF TX/POF 10/100-D	2832807	1
Interface module with 1 × twisted pair 10/100 Mbps in RJ45 format and 1 × HCS fiber 100 Mbps in F-SMA format for connection on the **bottom**	FL IF TX/HCS 100-D	2832739	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format for connection on the **bottom** and **parameterization memory**	FL IF MEM 2TX-D	2832483	1
Interface module with 2 × polymer fiber 10/100 Mbps in F-SMA format for connection on the **bottom**	FL IF 2POF 10/100-D	2832852	1
Interface module with 2 × HCS fiber 100 Mbps in F-SMA format for connection on the **bottom**	FL IF 2HCS 100-D	2832742	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format and **Power over Ethernet** for connection on the **front**	FL IF 2PSE-F	2832904	1
Interface module with 2 × polymer fiber 10/100 Mbps in SC-RJ format for connection on the **bottom** and **optical diagnostics**	FL IF 2POF SCRJ-D	2891084	1

Accessories

Description	Order Designation	Order No.	Pcs./Pck.
Converter board, which extends the FL IF TX/POF 100... interface module for use as a stand-alone media converter	FL CB IF	2832470	1
Labeling field for labeling the ports of the head station and extension modules	FL M LABEL	2891055	1
RJ45 connector with additional latching	VS-08-T-G-RJ45/IP20	1652295	5
Gray RJ45 connector set for linear cable	FL PLUG RJ45 GR/2	2744856	2
Green RJ45 connector set for crossed cable	FL PLUG RJ45 GN/2	2744571	2
Assembly tool for RJ45 connector	FL CRIMPTOOL	2744869	1
Factory Manager startup/diagnostic software	FL SWT	2831044	1
Network monitoring with HMI/SCADA systems	FL SNMP OPC SERVER	2832166	1
Patchbox 8 x RJ45 CAT 5e pre-assembled, can be retrofitted	FL PBX 8TX	2832496	1
Patchbox 6 x RJ45 CAT 5e and 4 SC-RJ, glass pre-assembled, can be retrofitted	FL PBX 6TX/4FX	2832506	1
Patch angle with two RJ45 network connections CAT5e including Layer 1 security elements	FL PF SEC 2TX	2832687	1
Patch angle with eight RJ45 network connections CAT5e including Layer 1 security elements	FL PF SEC 8TX	2832690	1
Patch angle with two RJ45 network connections CAT5e	FL PF 2TX CAT5E	2891165	1
Patch angle with eight RJ45 network connections CAT5e	FL PF 8TX CAT5E	2891178	1
Patch angle with two RJ45 network connections CAT6	FL PF 2TX CAT 6	2891068	1
Patch angle with eight RJ45 network connections CAT6	FL PF 8TX CAT 6	2891071	1
Patch cable, CAT 5, pre-assembled, 0.3 m long	FL CAT5 PATCH 0,3	2832250	10
Patch cable, CAT 5, pre-assembled, 0.5 m long	FL CAT5 PATCH 0,5	2832263	10
Patch cable, CAT 5, pre-assembled, 1.0 m long	FL CAT5 PATCH 1,0	2832276	10
Patch cable, CAT 5, pre-assembled, 1.5 m long	FL CAT5 PATCH 1,5	2832221	10
Patch cable, CAT 5, pre-assembled, 2.0 m long	FL CAT5 PATCH 2,0	2832289	10
Patch cable, CAT 5, pre-assembled, 3.0 m long	FL CAT5 PATCH 3,0	2832292	10
Patch cable, CAT 5, pre-assembled, 5.0 m long	FL CAT5 PATCH 5,0	2832580	10
Patch cable, CAT 5, pre-assembled, 7.5 m long	FL CAT5 PATCH 7,5	2832616	10
Patch cable, CAT 5, pre-assembled, 10.0 m long	FL CAT5 PATCH 10	2832629	10
Polymer fiber connectors (two duplex connectors in the set)	PSM-SET-SCRJ-DUP/2-POF	2708656	1
Polishing set for polymer fiber connectors (required to assemble polymer fiber connectors)	VS-SCRJ-POF-POLISH	1656673	1
Fiber optic polymer fiber cable for indoor installation	PSM-LWL-KDHEAVY	2744319	1
HCS fiber connectors (two duplex connectors in the set)	PSM-SET-SCRJ-DUP/2-HCS	2313070	1
Tool kit for HCS connectors (required to assemble HCS fiber connectors)	PSM-HCS-KONFTOOL/SCRJ	2708876	1
Fiber optic HCS cable for indoor installation	PSM-LWL-HCS-RUGGED-200/230	2799885	1
Fiber optic HCS cable for outdoor installation	PSM-LWL-HCSO-200/230	2799445	1

11.4 Ordering Data for GL-Certified Components (GL Certificate No. 24 2750 4 HH)

Products

Description	Order Designation	Order No.	Pcs./Pck.
Modular Managed Switch - head station	FL SWITCH MM HS/M	2832522	1
Extension module with 4 slots for eight ports	FL MXT/M	2832535	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format for connection on the **bottom** and **parameterization memory**	FL IF MEM 2TX-D	2832483	1
Interface module with 2 × glass fiber (multi-mode) 100 Mbps in SC format for connection on the **bottom**	FL IF 2FX SC-D	2832425	1
Interface module with 2 × glass fiber (single mode) 100 Mbps in SC format for connection on the **bottom**	FL IF 2FX SM SC-D	2832205	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format for connection on the **front**	FL IF 2TX VS-RJ-F	2832344	1
Interface module with 2 × twisted pair 10/100 Mbps in RJ45 format for connection on the **bottom**	FL IF 2TX VS-RJ-D	2832357	1

HOTLINE:

Should problems occur that cannot be resolved with the help of this documentation, please contact our hotline:

+49 - (0) 52 35 - 34 18 88

factoryline-service@phoenixcontact.com

A Appendix: Index

Symbols

"Private" password 4-18
% scale 4-37

Numerics

0.x.x.x addresses 3-5
127.x.x.x addresses 3-4
48 V supply 3-24
7-segment display 1-14

A

Access Control 4-19
Access Control for Web 4-20
Address combinations 3-4
Agent 4-41
Aging time 3-1, 4-31
Alarm contact 2-11
Allowed MAC Addresses 4-32
Alternate port 5-26
Analysis option 4-39
ANDing 3-5
Assembly 2-3
Assigning IP addresses 3-3
Assigning IP parameters 3-2
Assignment of F-SMA ports 3-13
Assignment of the RJ45 female connector 3-11
Auto crossing 3-9
Auto negotiation 3-9
Auto polarity 3-9

B

Bargraph 4-37
Basic switch configuration 4-118
Block 4-33
Block packets 4-31
Block packets with automatic reenabling 4-32
BootP 4-14
BootP reply 4-14
Bootstrap protocol 4-14
BPDU packets 3-32
Bridge MIB 4-40

C

Cable interrupt 3-10
Cascading style sheets Level 1 4-11
Change Password 4-18
Class 0 4-34
Class 4 4-34
Clear Memory Module 4-24
Configuration comparison 4-23
Configuration during booting 4-23
Configuration file 4-22
Connecting the 48 V PoE supply voltage 3-26
Connecting the F-SMA connectors 3-12
Connecting the RJ45 connectors 3-10
Connecting the SC-D connectors 3-17, 3-29
Connecting the ST connectors 3-18
Converter board 1-4
Counter states 4-28
CRC errors 3-31
Ctrl + L 4-116

D

Data bits 2-12
DCP 4-15
Default priority 3-32
Default settings 3-1
Default upon delivery 3-1
Designated port 5-26
Destination address 3-31
Destination address field 3-31
Destination port 4-31
Device replacement 4-23
DHCP 4-15
DHCP lease time 3-8
DHCP server 3-8
Diagnostic/status indicators 1-7
Dimensions of the
Modular Managed Switch System 1-10
DIP switch 3-13
Disconnected load 3-24
Discovery and Configuration Protocol 4-15
Display 4-35
Dotted decimal notation 3-3
Dotted notation 4-19

Dust protection caps 3-14
Dynamic Host Configuration Protocol 4-15

E

Edge port 5-26
EMC1 2-10
Engineering tool 4-15
Environmental Category EMC2 2-10
Error code "87" 3-22
Error states 2-11
Etherlike MIB 4-40
Event Table 4-37
Excel worksheet 4-39
Extension module 1-4
External management 2-12

F

Factory Manager 4-1
Far End Fault Detection 3-16, 3-18, 3-28
Faulty firmware 4-120
Faulty software 4-120
Fiber connection 3-15
Fiber type 3-17, 3-29
Firmware download 4-17
Firmware update 4-7
Firmware versions 1-5
FL IF 2FX SC 3-16, 3-28
FL IF 2FX SM SC 3-16
FL IF 2FX ST-D 3-18
FL IF 2HCS 100 3-14
FL IF 2POF 10/100 3-11
FL IF 2PSE-F 3-24
FL IF 2TX VS-RJ 3-9
FL IF MEM 2TX-D 3-22
FL IF TX/HCS 100 3-20
FL IF TX/POF 10/100 3-19
FL MXT/M 1-1
FL SWITCH MM HS/M 1-1
Floppy disk icon 4-11
Flow control 2-12
Flowchart Assigning IP parameters 3-8
Flowchart after a restart 3-7
Forgotten your password? 4-18
Forward delay 5-5
Fragments 3-31
Frame switching 3-31
Front view 1-8
F-SMA port 3-11
Function of the memory module 3-22
Function switch 1-7

G

GL 1-3
Glass fiber connection 3-17, 3-29
GL-certified operation 2-10, 3-9
Grounding 2-12

H

HCS connection 3-15
HCS port 3-14
Hello time 5-5
Host ID 3-3
Hot plugging 2-5
Hyper Text Transfer Protocol 4-11
HyperTerminal 4-116, 4-120

I

Iana-address-family MIB 4-40
IANAifType MIB 4-40
IEEE 802.1D 3-32
IEEE 802.1d 5-1
IEEE 802.1w 5-1
IEEE 802.3 3-11
If MIB 4-40
IGMP packets 3-32
Illegal access 4-31
Illegal Address Counter 4-24
Industrial RJ45 connector 3-10
IO controller 4-15
IP address 3-1
IP address assignment 4-14

J

JavaScript 1.2 4-11

L

Large tree support 5-5
Last Source MAC Address 4-33
Learning addresses 3-31
LEDs 1-12
Line monitoring 3-10
Link monitoring 4-25

Link test pulse 3-10
Load the last stored configuration 4-22
Loading the configuration data 3-7
Login screen 4-117
Logout 4-12

M

MAC address 3-31
MAC Address Table 4-39
Management Information Base 4-40, 4-41
Management via local V.24 (RS-232) communication interface 4-116
Management via Telnet 4-123
Maximum Age of STP Information 5-5
Memory Module 4-23
MIB 4-40
MIB 2 4-40
Mini-DIN female connector 2-12
Mini-DIN format 4-116
Modular structure 1-2
Multi-address function 3-31
Multicast data packets 4-31
Multicast/broadcast address 3-31

N

Navigation tree 4-12
NEF 1- 6 2-10
Network availability 1-2
Network class 3-3
Network ID 3-3
Network part 3-5
Network topology 5-2
No redundancy 5-3

O

Online diagnostics 4-36
Overload 3-24

P

P bridge MIB 4-40
Packet processing sequence 3-32
Parameterization memory default upon delivery 3-22
Parity 2-12
Password 4-11, 4-12
Password concept 4-12
PoE configuration 4-34
PoE interface 3-24
PoE interface module 4-34
PoE Port Table 4-33
POF connection between devices 3-12
POF interface 3-12
Point-to-point connection 4-23
Polymer fiber optic paths 3-13
Polymer/HCS fibers 1-1
Port assignment 1-12
Port capacity 4-31
Port Configuration Table 4-25
Port Mirroring 4-31
Port prioritization 3-32
Port roles 5-26
Port Security 4-31
Port security status 4-24
Port switched off 4-26
Port Table 4-25
Port-based prioritization of data streams 3-32
Positive latches 2-3
Power over Ethernet Port Table 4-33
Prioritization 3-32
Priority field 3-32
Priority level 3-32
Priority queues 3-32
Private MIBs 4-68
Processing rules 3-32
PROFINET 4-15
PROFINET connection 4-15
Protective caps 3-14
pxcFactoryLine 4-68
pxcGlobal 4-68
pxcModules 4-68

Q

Q bridge MIB 4-40

R

Rapid Reconfiguration Spanning Tree 5-1
Rapid Spanning Tree Protocol 5-1
Read/write access 4-19
Read-only access 4-19
Reboot 4-24
Receive queue 3-32
Redundancy mechanism 5-2
Redundant 24 V DC supply 2-9

Redundant data paths 5-1
Refresh interval..... 4-18
Removal..... 2-3
Request 4-14
Required hardware 1-6
Resetting to the default settings 4-119, 4-125
RFC1213 4-40
RFC1213 MIB 4-45
RMON MIB 4-40
Root 5-1
Root port 5-26
RSTP MIB..... 4-40

S

Save current configuration..... 4-21
Saving the firmware 4-17
Security mode..... 4-31
Set default upon delivery 4-21
Shipbuilding 1-3
Simple Network Management Protocol 4-40
SNMP 4-40
SNMP interface..... 4-40
SNMP objects 4-40
SNMP-FRAMEWORK MIB 4-40
SNMPv2 MIB 4-40
Software Update 4-17
Source and destination addresses 3-31
Source port 4-31
Special IP addresses 3-4
Standard browsers..... 4-11
Starting with faulty software..... 4-120
States for "Status of current configuration" 4-21
Static assignment 4-14
Stop bits..... 2-12
Store-and-forward mode..... 3-31
STP..... 5-1
Strict Priority 3-33
Structure of the subnet mask..... 3-5
Subnet mask..... 3-1
Subnet masks 3-5
Subnetwork router 3-5
Supply voltage 2-9
Surge voltage/undervoltage..... 3-24
Switch position..... 3-13
Switch station..... 4-24
System bus firmware 3-22

T

Tagging..... 3-33
Telnet client 4-123
Telnet protocol..... 4-123
Telnet server..... 4-123
Telnet terminals 4-123
Terminal emulation 2-12
Termination devices..... 4-32
TFTP server..... 4-7
Thermal error..... 3-24
Traffic classes..... 3-32, 3-33
Transmission power..... 3-13
Trap Configuration..... 4-16
Trap only..... 4-31
Trap receiver..... 4-16
Trap targets/receivers..... 4-41
Traps..... 4-41
Tree structure 5-1
Tree structure of the MIB..... 4-44

U

Unauthorized access attempts 4-24
Unicast addresses 3-32
User interface 4-124
User Interfaces 4-18
User interfaces..... 4-117
Using the VS-08-T-G-RJ45/IP20 3-10
Utilization 4-37

V

V.24 (RS-232) interface..... 2-12
Valid IP parameters 3-2
VLAN ID..... 4-39
VLAN/priority tag..... 3-32
VS-08-T-G-RJ45/IP20 3-10
VT100 terminal 2-12

W

WBM..... 4-11
Web server 4-11
Web-based management 4-11

X

XMODEM ready..... 4-121